



7450 Ethernet Service Switch
7750 Service Router
7950 Extensible Routing System
Virtualized Service Router
Release 23.10.R1

Peering Quick Reference Guide

3HE 19853 AAAA TQZZA 01
Edition: 01
October 2023

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

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

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

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

No part of this document may be modified.

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

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

© 2023 Nokia.

Table of contents

1	Getting started.....	5
1.1	About this guide.....	5
1.2	Conventions.....	5
1.2.1	Precautionary and information messages.....	6
1.2.2	Options or substeps in procedures and sequential workflows.....	6
2	Peering configuration process.....	7
2.1	Introduction.....	8
2.2	Topology.....	8
3	Hardware configuration.....	9
3.1	Configuring line cards.....	9
3.2	Configuring ports and interfaces.....	9
4	Configuring routing protocols.....	12
4.1	IGP – OSPF.....	12
4.2	IGP – IS-IS.....	12
4.3	BGP.....	13
5	Configuring peering.....	16
5.1	Route policies.....	16
5.2	Cflowd.....	18
5.3	RPKI for prefix origin validation.....	19
5.4	BGP FlowSpec.....	20
5.5	uRPF.....	20
6	Configuring system and routing security.....	22
6.1	CPM filters.....	22
6.2	Management Access Filter.....	23
6.3	ACLs.....	25
6.3.1	Rate limiting DDoS traffic.....	26
6.3.2	Redirecting suspicious traffic.....	26
6.3.3	ACL show commands.....	27
6.4	PBR.....	27

7	Configuring QoS.....	29
7.1	Classification.....	29
7.2	Queuing.....	29
7.3	Scheduling.....	30
7.4	Re-marking.....	30
8	Additional system configuration.....	31
8.1	Switching from the classic CLI to the MD-CLI.....	31
8.2	User and profile management.....	31
8.3	NTP.....	32
8.4	System alarms and logging.....	32
9	Appendix A: Custom CLI commands (pySROS).....	33
10	Appendix B: Configuration groups.....	34

1 Getting started

1.1 About this guide

This guide provides the basic configuration required to set up a Nokia router as a peering router. The examples in this guide cover all features required for the peering function.



Note: This guide does not provide detailed information about peering features. Users are expected to have a basic understanding about these features. For detailed information, see the SR OS customer documentation [WebHelp](#) or the [Nokia Doc Center](#).

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.



Note: Unless otherwise indicated, this guide uses MD-CLI command syntax and configuration examples.

The topics and commands described in this document apply to the:

- 7450 ESS
- 7750 SR
- 7950 XRS
- Virtualized Service Router (VSR)

For a list of unsupported features by platform and chassis, see the *SR OS R23.x.Rx Software Release Notes*, part number 3HE 19269 000 x TQZZA.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.



Note: The SR OS CLI trees and command descriptions can be found in the following guides:

- *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*
- *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide* (for both the MD-CLI and classic CLI)
- *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*



Note: This guide generically covers Release 23.x.Rx content and may contain some content that is released in later maintenance loads. See the *SR OS R23.x.Rx Software Release Notes*, part number 3HE 19269 000 x TQZZA, for information about features supported in each load of the Release 23.x.Rx software.

1.2 Conventions

This section describes the general conventions used in this guide.

1.2.1 Precautionary and information messages

The following information symbols are used in the documentation.



DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.



WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.



Caution: Caution indicates that the described activity or situation may reduce your component or system performance.



Note: Note provides additional operational information.



Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step.
 - This is one option.
 - This is another option.
 - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
 - a. This is one substep.
 - b. This is another substep.

2 Peering configuration process

The following table lists the SR OS peering configuration tasks. Information in this guide is presented in an overall logical configuration flow. Each section describes a software area and provides the MD-CLI command usage to configure commands for the functional area.

Table 1: Configuration process

Area	Task	Section
Peering configuration introduction	Introduction to peering	Introduction to peering
	Peering topology	Peering configuration topology
Hardware configuration	Configure line cards	Configuring line cards
	Configure ports and interfaces	Configuring ports and interfaces
Routing protocols configuration	Configure an IGP	IGP – OSPF IGP – IS-IS
	Configure BGP	BGP
Peering configuration	Configure route policies	Route policies
	Configure cflowd	Cflowd
	Configure RPKI for prefix origin validation	RPKI for prefix origin validation
	Configure FlowSpec	BGP FlowSpec
	Configure uRPF	uRPF
System and routing security configuration	Configure CPM filters	CPM filters
	Configure management access filter	Management Access Filter
	Configure ACLs	ACLs
	Configure rate limiting for DDoS traffic	Rate limiting DDoS traffic
	Configure redirecting suspicious traffic	Redirecting suspicious traffic
	Run ACL show commands	ACL show commands
QoS configuration	Configure classification	Classification
	Configure queuing	Queuing
	Configure scheduling	Scheduling

Area	Task	Section
	Configure re-marking	Re-marking
Additional system configuration (optional)	Switching from the classic to the MD-CLI	Switching from the classic CLI to the MD-CLI
	User and profile management	User and profile management
	Configure NTP	NTP
	Configure system alarms and logging	System alarms and logging
Appendix A	Configure custom CLI commands (pySROS)	Appendix A: Custom CLI commands (pySROS)
Appendix B	Configure configuration groups	Appendix B: Configuration groups

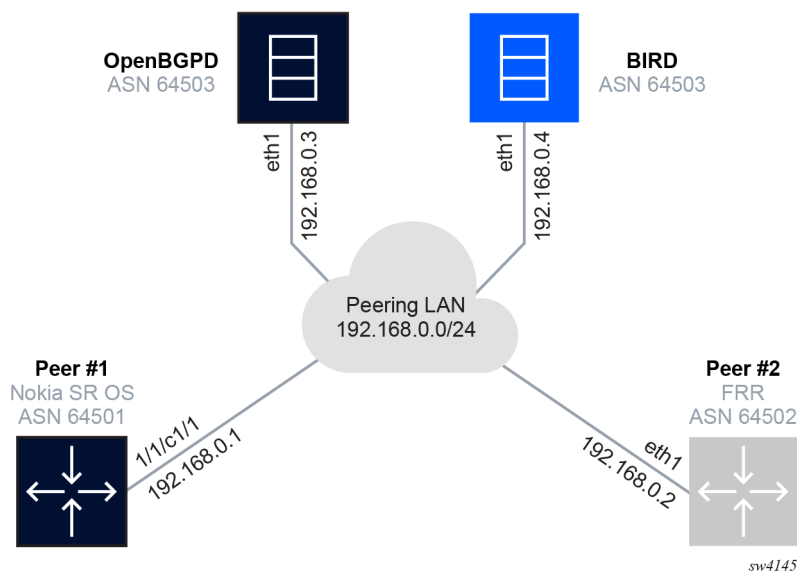
2.1 Introduction

Peering is an agreement established between two networks or two Autonomous Systems (ASs) to exchange routing information using the BGP protocol as described in this guide.

2.2 Topology

The configuration examples in this guide display the connection of the Peer #1 Nokia SR OS ASN 64501 router (shown in the following figure) as a peering router to the rest of the network.

Figure 1: Peering topology



3 Hardware configuration

The following sections describe the hardware configurations.

3.1 Configuring line cards

Define line card types explicitly based on the system type.

Example: Configuring line card type configuration for the 7750 SR-1 with one pluggable MDA card

```
configure card 1 card-type iom-1
configure card 1 level he
configure card 1 mda 1 mda-type me6-100gb-qsfp28
```

Use the following command to show the operational status of the card.

```
show card state
```

Example: Card state output

```
=====
Card State
=====
Slot/  Provisioned Type      Admin Operational  Num   Num  Comments
Id      Equipped Type (if different) State State           Ports MDA
-----
1       iom-1:he                up   up                2
1/1    me6-100gb-qsfp28       up   up                6
A       cpm-1                    up   up                Active
=====
```

3.2 Configuring ports and interfaces

Configure the physical port first, followed by an interface with an IPv4 or IPv6 address.

Each port is considered a connector that supports breakout. Configure the connector with the breakout type so that the appropriate ports are created and can be configured.

Example: Configuring the connector breakout type

The following example displays the configuration of a connector breakout. The default port MTU value is 9212.

```
configure port 1/1/c1 admin-state enable
configure port 1/1/c1 connector { breakout c1-100g }
configure port 1/1/c1/1 admin-state enable
```

```
configure port 1/1/c1/1 description "To Peering LAN"
```

Example: Configuring the router interface

The interface is provided a name, an IP address, and is associated with a physical port as shown in the following example.

```
configure router "Base" interface "To-Peering-LAN" port 1/1/c1/1
configure router "Base" interface "To-Peering-LAN" ipv4 { primary address 192.168.0.1
prefix-length 24 }
configure router "Base" interface "To-Peering-LAN" ipv6 { address 2001:a8::4 prefix-length
124 }
```

Example: Configuring the system interface

The system interface is the router's loopback interface (like lo0 or loopback0) and is configured as shown in the following example.

```
configure router "Base" interface "system" ipv4 { primary address 10.0.0.1 prefix-length
32 }
configure router "Base" interface "system" ipv6 { address 2001:1::101 prefix-length 128 }
```

Use the following command to display the port information.

```
show port
```

Example: Port status output

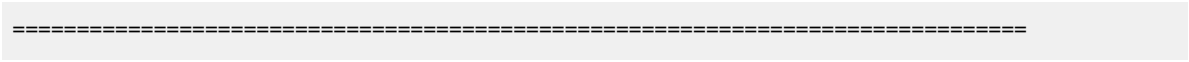
```
=====
Ports on Slot 1
=====
Port      Admin Link Port   Cfg  Oper  LAG/  Port  Port  Port  C/QS/S/XFP/
Id        State  State State  MTU  MTU  Bndl  Mode  Encp  Type  MDIMDX
-----
1/1/c1    Up     Link  Link  Up
1/1/c1/1  Up     Yes  Up    9212 9212  - netw null cgige
=====
```

Use the following command to display the router IP interface information.

```
show router interface
```

Example: Router interface status output

```
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm    Opr(v4/v6)  Mode    Port/SapId
IP-Address          PfxState
-----
To-Peering-LAN      Up     Up/Up       Network 1/1/c1/1
192.168.0.1/24      n/a
2001:a8::4/124      n/a
fe80::1668:ffff:fe00:0/64  n/a
system              Up     Up/Up       Network system
10.0.0.1/32         n/a
2001:1::101/128     n/a
-----
Interfaces : 2
=====
```



4 Configuring routing protocols

Configure an IGP protocol (OSPF or IS-IS) to connect the router to other network elements within the same AS. BGP is used to establish the peering session with the external router.

4.1 IGP – OSPF

The following example displays the OSPF configuration to connect with a router R1 within the same AS. The port and interface configuration for this connection can be configured as described in [Configuring ports and interfaces](#).

For more information about OSPF configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*.

Example: Configuring OSPF

```
configure router "Base" ospf 0 admin-state enable
configure router "Base" ospf 0 area 0.0.0.0 { interface "Interface-to-R1" interface-type
point-to-point }
```

Use the following command to display OSPF neighbor information.

```
show router ospf neighbor
```

Example: OSPF neighbor information output

```
=====
Rtr Base OSPFv2 Instance 0 Neighbors
=====
Interface-Name          Rtr Id          State          Pri  RetxQ  TTL
  Area-Id
-----
Interface-to-R1        10.10.20.103   Full           1    0      35
  0.0.0.0
-----
No. of Neighbors: 1
=====
```

4.2 IGP – IS-IS

The following example displays the configuration to establish IS-IS adjacency with a router R1 within the same AS. The router is set to IS-IS Level 2 and native IPv6 routing is enabled. The port and interface configuration for this connection can be configured as described in [Configuring ports and interfaces](#).

For more information about IS-IS configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*.

Example: Configuring IS-IS

```

configure router "Base" isis 0 admin-state enable
configure router "Base" isis 0 ipv6-routing native
configure router "Base" isis 0 level-capability 2
configure router "Base" isis 0 system-id 0100.0000.0001
configure router "Base" isis 0 area-address [49.0000]
configure router "Base" isis 0 interface "Interface-to-R1" { interface-type point-to-point }

```

Use the following command to display IS-IS neighbor information.

```
show router isis adjacency
```

Example: IS-IS adjacency status output

```

=====
Rtr Base ISIS Instance 0 Adjacency
=====
System ID                Usage State Hold Interface          MT-ID
-----
sr103                    L2   Up   25   Interface-to-R1          0
-----
Adjacencies : 1
=====

```

4.3 BGP

In the following example, the External Border Gateway Protocol (EBGP) session is configured using the interface IP as the neighbor IP. The local AS is configured as 64501 and remote AS is 64503.

For more information about BGP configuration, see the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR Unicast Routing Protocols Guide*.

Example: Configuring an EBGP session

```

configure router "Base" autonomous-system 64501
configure router "Base" bgp router-id 10.0.0.1
configure router "Base" bgp group "eBGP-Peering" { type external }
configure router "Base" bgp group "eBGP-Peering" { peer-as 64503 }
configure router "Base" bgp group "eBGP-Peering" { family ipv4 true }
configure router "Base" bgp group "eBGP-Peering" { family ipv6 true }
configure router "Base" bgp neighbor "192.168.0.3" { group "eBGP-Peering" }
configure router "Base" bgp neighbor "192.168.0.4" { group "eBGP-Peering" }

```

Use the following command to display BGP neighbor status.

```
show router bgp summary
```

Example: BGP neighbor status summary output

```

=====
BGP Router ID:10.0.0.1      AS:64501      Local AS:64501
=====
BGP Admin State           : Up      BGP Oper State           : Up

```

```

Total Peer Groups      : 1          Total Peers           : 2
Total VPN Peer Groups : 0          Total VPN Peers       : 0
Current Internal Groups : 1        Max Internal Groups   : 1
Total BGP Paths        : 21         Total Path Memory     : 7416

```

```
...
```

```
=====
BGP Summary
=====
```

```
Legend : D - Dynamic Neighbor
=====
```

```
Neighbor
Description
          AS PktRcvd InQ Up/Down State|Rcv/Act/Sent (Addr Family)
          PktSent OutQ
-----
192.168.0.3
          64503      20   0 00h07m26s 3/0/0 (IPv4)
          19         0   0/0/0 (IPv6)
192.168.0.4
          64503      27   0 00h10m05s 2/0/0 (IPv4)
          41         0   1/0/0 (IPv6)
-----
```

Use the following command to display routes received from a neighbor.

```
show router bgp neighbor 2001:a8::5 received-routes
```

Example: Routes received from a neighbor output

```
=====
BGP Router ID:10.0.0.1      AS:64501      Local AS:64501
=====
Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
               l - leaked, x - stale, > - best, b - backup, p - purge
Origin codes  : i - IGP, e - EGP, ? - incomplete
=====
BGP IPv4 Routes
=====
Flag  Network                LocalPref  MED
      Nexthop (Router)      Path-Id    IGP Cost
      As-Path                Label
-----
i     10.10.1.24/29           n/a        None
      192.168.0.3           None        0
      64503                  -
i     10.10.20.103/32        n/a        None
      192.168.0.3           None        0
      64503                  -
i     192.168.0.0/24         n/a        None
      192.168.0.3           None        0
      64503                  -
-----
Routes : 3
=====
```

Use the following command to display the number of routes installed per line card summary output.

```
show router fib 1 summary ipv4
```

Example: Number of routes installed per line card summary output

```
=====
FIB Summary
=====
                                Active
-----
Static                          0
Direct                          3
Host                             0
BGP                             0
BGP VPN                         0
--snip--
VPN Leak                         0
-----
Total Installed                  4
-----
Current Occupancy                1%
Overflow Count                   0
Suppressed by Selective FIB      0
Occupancy Threshold Alerts
  Alert Raised 0 Times;
=====
```

5 Configuring peering

This section provides configuration examples for peering features. Not all features are required to set up a basic peering connection.

5.1 Route policies

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

The following examples configure AS path and community lists that can be referenced by multiple policies.

Regular expression strings can be used to specify match criteria for the AS path and communities. For more information about using regular expressions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*.

Example: Configuring AS path and community lists

Regular expression strings are used to specify match criteria for the AS path and communities in the following example.

```
configure policy-options as-path "PEERING" { expression "64503" }
configure policy-options as-path-group "BOGON" { entry 10 expression ".* 0 .*" }
configure policy-options as-path-group "BOGON" { entry 20 expression ".* [64496-64511] .*" }
configure policy-options as-path-group "BOGON" { entry 30 expression ".* 65535 .*" }

configure policy-options community "LARGE-PEER" { member "65100:100" }
configure policy-options community "SMALL-PEERS" { member "65200:200" }
configure policy-options community "SMALL-PEERS" { member "65400:.*$" }
configure policy-options community "SMALL-PEERS" { member "65500:.*" }
```

Example: Configuring prefix lists

```
configure policy-options prefix-list "AS65xx-prefixes" { prefix 10.100.100.0/24 type longer }
configure policy-options prefix-list "AS65xx-prefixes" { prefix 10.200.0.0/16 type through through-length 24 }
configure policy-options prefix-list "AS65xx-prefixes" { prefix 192.168.10.0/24 type through through-length 24 }
configure policy-options prefix-list "AS65xx-prefixes" { prefix 10.10.1.1/32 type exact }
configure policy-options prefix-list "AS65xx-prefixes" { prefix 172.16.0.0/16 type range start-length 16 }
configure policy-options prefix-list "AS65xx-prefixes" { prefix 172.16.0.0/16 type range end-length 19 }
configure policy-options prefix-list "IPv6-list" { prefix 2001:fd00:84::/46 type longer }
configure policy-options prefix-list "SMALLER_THAN_/48" { prefix ::/0 type range start-length 49 }
configure policy-options prefix-list "SMALLER_THAN_/48" { prefix ::/0 type range end-length 128 }
```


Example: Configuring policy statements

The following example displays a policy statement configuration. Entries can be either numbered or named.

```
configure policy-options policy-statement "EXT-AS-IMPORT" entry-type named
configure policy-options policy-statement "EXT-AS-IMPORT" named-entry "Routes-
AS64503" { from as-path name "PEERING" }
configure policy-options policy-statement "EXT-AS-IMPORT" named-entry "Routes-
AS64503" { action action-type accept }
```

The policy can be applied as import or export under the BGP router, group, or neighbor context.

Example: Importing policy under BGP root

```
configure router "Base" bgp group "eBGP-Peering" import { policy ["EXT-AS-IMPORT"] }
```

Test and evaluate route policies

Route policies can be tested and evaluated before they are applied to BGP as shown in the following example.

For more information about Route Policy Testing commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide*.

Use the following command to test and evaluate route policies.

```
show router bgp policy-test plcy-or-long-expr "EXT-AS-IMPORT" family ipv4 prefix 0.0.0.0/0
longer neighbor 192.168.0.3
```

Example: Testing and evaluating route policies output

```
=====
BGP Router ID:10.0.0.1          AS:64501          Local AS:64501
=====
Legend -
Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
                l - leaked, x - stale, > - best, b - backup, p - purge
Origin codes  : i - IGP, e - EGP, ? - incomplete
=====
BGP IPv4 Routes
=====
```

Network Nexthop As-Path	LocalPref Path-Id	MED Label
Accepted by Policy EXT-AS-IMPORT Entry Routes-AS64503		
10.10.1.24/29	None	None
192.168.0.3 64503	None	n/a -
Accepted by Policy EXT-AS-IMPORT Entry Routes-AS64503		
10.10.20.103/32	None	None
192.168.0.3 64503	None	n/a -
Accepted by Policy EXT-AS-IMPORT Entry Routes-AS64503		
192.168.0.0/24	None	None
192.168.0.3 64503	None	n/a -

```
-----
```

```
Routes : 3
=====
```

5.2 Cflowd

Cflowd is a tool used to obtain samples of IPv4, IPv6, MPLS, and Ethernet traffic data flows through a router. For more information about cflowd, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

Example: Configuring cflowd

```
configure cflowd overflow 10
configure cflowd active-flow-timeout 30
configure cflowd inactive-flow-timeout 10
configure cflowd sample-profile 1 { }
configure cflowd sample-profile 1 { sample-rate 100 }

configure cflowd collector 10.10.10.2 port 5000 { description "Neighbor collector" }
configure cflowd collector 10.10.10.2 port 5000 { autonomous-system-type peer }
configure cflowd collector 10.10.10.2 port 5000 { version 8 }
configure cflowd collector 10.10.10.2 port 5000 { aggregation protocol-port true }
configure cflowd collector 10.10.10.2 port 5000 { aggregation source-destination-prefix true }

configure cflowd collector 10.10.10.9 port 2000 { description "v9collector" }
configure cflowd collector 10.10.10.9 port 2000 { template-set mpls-ip }
configure cflowd collector 10.10.10.9 port 2000 { version 9 }
configure router "Base" interface "To-Peering-LAN" cflowd-parameters { sampling unicast type interface }
```

Use the following command to display the basic information about the administrative and operational status of cflowd.

```
show cflowd status
```

Example: Cflowd status output

```
=====
Cflowd Status
=====
Cflowd Admin Status   : Enabled
Cflowd Oper Status   : Enabled
Cflowd Export Mode    : Automatic
Active Flow Timeout   : 30 seconds
---snip---

Active Flows          : 0
Dropped Flows         : 0
Total Pkts Rcvd       : 0
Total Pkts Dropped    : 0
Overflow Events       : 0

Raw Flow Counts      Aggregate Flow Counts
Flows Created         0                0
Flows Matched         0                0
Flows Flushed         0                0
=====
```

```

Sample Profile Info
=====
Profile Id      Sample Rate
-----
      1              100
=====
Version Info
=====
Version Status          Sent          Open          Errors
-----
      5 Disabled              0              0              0
      8 Enabled              0              0              0
      9 Enabled              0              0              0
     10 Disabled              0              0              0
=====

```

5.3 RPKI for prefix origin validation

7750 SR supports Resource Public Key Infrastructure (RPKI) for BGP prefix origin validation.

For more information about BGP prefix origin validation, see the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR Unicast Routing Protocols Guide*.

Example: BGP prefix origin validation in a RPKI session

```

configure router "Base" origin-validation rpki-session 172.31.1.2 admin-state enable
configure router "Base" origin-validation rpki-session 172.31.1.2 local-address 10.10.1.4
configure router "Base" origin-validation rpki-session 172.31.1.2 port 8282

configure router "Base" bgp group "eBGP-Peering" origin-validation { ipv4 true }
configure router "Base" bgp group "eBGP-Peering" origin-validation { ipv6 true }

configure router "Base" bgp best-path-selection { origin-invalid-unusable true }

```

Use the following command to display RPKI session information.

```
show router origin-validation rpki-session detail
```

Example: RPKI session status detail output

```

=====
RPKI Session Information
=====
IP Address       : 172.31.1.2
Description      : (Not Specified)
-----
Port             : 8282                Oper State      : connect
Uptime          : 0d 00:00:00          Flaps           : 0
Active IPv4 Records: 0                Active IPv6 Records: 0
Admin State     : Up                  Local Address    : 10.10.1.4
Hold Time      : 600                  Refresh Time     : 300
Stale Route Time : 3600                Connect Retry    : 120
Serial ID      : 0                    Session ID       : 0
=====
No. of Sessions : 1
=====

```

5.4 BGP FlowSpec

FlowSpec is a standardized method for using BGP to distribute traffic flow specifications (flow routes) throughout a network. FlowSpec is supported for both IPv4 and IPv6.

For more information about FlowSpec, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*.

Example: FlowSpec configuration

```
configure router "Base" bgp neighbor "192.168.0.3" family ipv4 ipv6 flow-ipv4 flow-ipv6
true

configure filter ip-filter "FSPEC-filter" default-action accept
configure filter ip-filter "FSPEC-filter" filter-id 99
configure filter ip-filter "FSPEC-filter" embed { flowspec offset 1000 }
configure filter ip-filter "FSPEC-filter" embed { flowspec offset 1000 router-instance
"Base" }

configure router "Base" interface "To-Peering-LAN" ingress { filter ip "FSPEC-filter" }
```

Use the following command to display BGP flow IPv4 routes.

```
show router bgp routes flow-ipv4
```

Use the following command to display IPv4 filter information.

```
show filter ip "FSPEC-filter"
```

Example: IP FPSEC filter output

```
=====
IP Filter
=====
Filter Id           : 99                               Applied           : Yes
Scope              : Template                       Def. Action       : Forward
Type               : Normal
Shared Policer     : Off
System filter      : Unchained
Radius Ins Pt      : n/a
CrCtl. Ins Pt      : n/a
RadSh. Ins Pt      : n/a
PccRl. Ins Pt      : n/a
Entries            : 0
Description        : (Not Specified)
Filter Name        : FSPEC-filter
-----
Filter Match Criteria : IP
-----
No Match Criteria Found
=====
```

5.5 uRPF

Unicast reverse path forwarding check (uRPF) helps to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. The uRPF feature is supported for both IPv4 and IPv6 on network and access.

For more information about uRPF, see the 7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide.

Example: uRPF configuration

```
configure router "Base" interface "To-Peering-LAN" ipv4 { urpf-check mode loose }
configure router "Base" interface "To-Peering-LAN" ipv6 { urpf-check mode loose }
```

6 Configuring system and routing security

To configure the system and routing security for peering, users can configure CPM filters, Management Access Filters (MAF), Access Control List filters (ACL), and Policy-based Routing (PBR).

6.1 CPM filters

CPM filters are hardware-based filters used to restrict traffic from the line cards directed to the CPM, such as control and management packets. Separate configuration is required for IPv4 and IPv6 packet matching conditions. Use prefix lists for groups of IP addresses.

For more information about CPM filters, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.



Note: Before committing the changes, make sure all IP addresses communicating with the router are included in the prefix list. The other option is to change the "entry 1000" action to "accept" for testing purposes.



Note: Use the **commit confirm** command to avoid getting locked out of the router.

Example: Configuring IPv4 CPM filters

The following example contains three entries. The third entry logs and drops all unmatched packets not explicitly treated by the first two entries.

```
configure filter match-list { ip-prefix-list "SNMP-Source" prefix 192.168.10.30/32 }
configure filter match-list { ip-prefix-list "SSH-Sources" prefix 10.10.100.10/32 }
configure filter match-list { ip-prefix-list "SSH-Sources" prefix 172.16.20.0/24 }
configure system security cpm-filter ip-filter { admin-state enable }
configure system security cpm-filter ip-filter { entry 100 description "SSH Access" }
configure system security cpm-filter ip-filter { entry 100 match protocol tcp }
configure system security cpm-filter ip-filter { entry 100 match src-ip ip-prefix-list
"SSH-Sources" }
configure system security cpm-filter ip-filter { entry 100 match dst-port eq 22 }
configure system security cpm-filter ip-filter { entry 100 action accept }
configure system security cpm-filter ip-filter { entry 200 description "SNMP Access" }
configure system security cpm-filter ip-filter { entry 200 match protocol udp }
configure system security cpm-filter ip-filter { entry 200 match src-ip ip-prefix-list
"SNMP-Source" }
configure system security cpm-filter ip-filter { entry 200 match dst-port eq 161 }
configure system security cpm-filter ip-filter { entry 200 action accept }
configure system security cpm-filter ip-filter { entry 1000 log 101 }
configure system security cpm-filter ip-filter { entry 1000 action drop }
```

Example: Configuring IPv6 CPM filters

```
configure filter match-list { ipv6-prefix-list "EBGP-v6-PEERS" prefix 2001:a8::4/127 }
configure filter match-list { ipv6-prefix-list "EBGP-v6-PEERS" prefix 2013:ab33:1::54/
127 }
```

```

configure system security cpm-filter ipv6-filter { admin-state enable }
configure system security cpm-filter ipv6-filter { entry 700 description "Inbound eBGP
IPv6 peers" }
configure system security cpm-filter ipv6-filter { entry 700 match next-header tcp }
configure system security cpm-filter ipv6-filter { entry 700 match src-ip ipv6-prefix-list
"EBGP-v6-PEERS" }
configure system security cpm-filter ipv6-filter { entry 700 match dst-port eq 179 }
configure system security cpm-filter ipv6-filter { entry 700 action accept }

configure system security cpm-filter ipv6-filter { entry 750 description "Outbound eBGP
IPv6 peers" }
configure system security cpm-filter ipv6-filter { entry 750 match next-header tcp }
configure system security cpm-filter ipv6-filter { entry 750 match src-ip ipv6-prefix-list
"EBGP-v6-PEERS" }
configure system security cpm-filter ipv6-filter { entry 750 match src-port eq 179 }
configure system security cpm-filter ipv6-filter { entry 750 action accept }

```

Use the following command to display CPM IPv6 filter information,

```
show system security cpm-filter ip-filter entry 1000
```

Example: CPM filter entry output

```

=====
CPM IP Filter Entry
=====
Entry Id          : 1000
Description       : (Not Specified)
-----
Filter Entry Match Criteria :
-----
Log Id           : 101
Src. IP          : n/a
Src. Port        : n/a
Dst. IP          : n/a
Dest. Port       : n/a
Protocol         : none           Dscp           : Undefined
ICMP Type        : Undefined      ICMP Code       : Undefined
Fragment         : Off            Option-present  : Off
IP-Option        : n/a            Multiple Option : Off
TCP-syn          : Off            TCP-ack        : Off
Action           : Forward
Match Router ID  : n/a
Dropped pkts    : 0                Forwarded pkts : 0
=====

```

6.2 Management Access Filter

The CPM uses Management Access Filters (MAFs) to perform filtering that applies to both traffic from the line cards directed to the CPM's CPU, as well as traffic from the management Ethernet port. Separate configuration is required for IPv4 and IPv6 packet matching conditions.

Prefix lists can be used for groups of IP addresses.

For more information about MAFs, see the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR System Management Guide*.

The following example shows three entries. The third entry logs and drops all unmatched packets not explicitly treated by the first two entries.



Note: Before committing the changes, make sure all IP addresses communicating with the router are included in the prefix list. The other option is to change the "entry 1000" action to "accept" for testing purposes.



Note: Use the **commit confirm** command to avoid being locked out of the router.

Example: Configuring IPv4 MAFs

```
configure system security management-access-filter ip-filter { default-action drop }
configure system security management-access-filter ip-filter { entry 100 description
  "Permit SSH Prefix" }
configure system security management-access-filter ip-filter { entry 100 action accept }
configure system security management-access-filter ip-filter { entry 100 match router-
instance "management" }
configure system security management-access-filter ip-filter { entry 100 match protocol
tcp }
configure system security management-access-filter ip-filter { entry 100 match src-ip ip-
prefix-list "SSH-Sources" }
configure system security management-access-filter ip-filter { entry 100 match mgmt-port
cpm }
configure system security management-access-filter ip-filter { entry 100 match dst-port
port 22 }
configure system security management-access-filter ip-filter { entry 200 description
  "Permit SNMP Prefix" }
configure system security management-access-filter ip-filter { entry 200 action accept }
configure system security management-access-filter ip-filter { entry 200 match router-
instance "management" }
configure system security management-access-filter ip-filter { entry 200 match protocol
udp }
configure system security management-access-filter ip-filter { entry 200 match src-ip ip-
prefix-list "SNMP-Source" }
configure system security management-access-filter ip-filter { entry 200 match mgmt-port
cpm }
configure system security management-access-filter ip-filter { entry 200 match dst-port
port 161 }
configure system security management-access-filter ip-filter { entry 2000 description
  "Management Plane Default" }
configure system security management-access-filter ip-filter { entry 2000 action drop }
configure system security management-access-filter ip-filter { entry 2000 log-events
true }
configure system security management-access-filter ip-filter { entry 2000 match router-
instance "management" }
configure system security management-access-filter ip-filter { entry 2000 match mgmt-port
cpm }
```

Example: Configuring IPv6 MAFs

The following example displays the configuration of MAF IPv6 filters.

```
configure filter match-list { ipv6-prefix-list "EBGP-v6-PEERS" prefix 2001:a8::4/127 }
configure filter match-list { ipv6-prefix-list "EBGP-v6-PEERS" prefix 2013:ab33:1::54/
127 }

configure system security management-access-filter ipv6-filter default-action drop
configure system security management-access-filter ipv6-filter entry 10 { match router-
instance "management" }
configure system security management-access-filter ipv6-filter { entry 10 action accept }
```



```

configure system security management-access-filter ipv6-filter entry 10 { match mgmt-port
  cpm }
configure system security management-access-filter ipv6-filter { entry 10 match next-
header tcp-udp }
configure system security management-access-filter ipv6-filter { entry 10 match src-ip
  ipv6-prefix-list "EBGP-v6-PEERS" }

configure system security management-access-filter ipv6-filter entry 1000 { action
  accept }
configure system security management-access-filter ipv6-filter entry 1000 { match router-
instance "management" }
configure system security management-access-filter ipv6-filter entry 1000 { match mgmt-
port cpm }

```

Use the following command to display management-access IP filters.

```
show system security management-access-filter ip-filter entry 2000
```

Example: IPv4 MAF output

```

=====
IPv4 Management Access Filter
=====
filter type      : ip
Def. Action      : deny
Admin Status     : enabled (no shutdown)
-----
Entry           : 2000
Description      : Management Plane Default
Src-ip          : undefined
Mgmt-port       : cpm
Protocol        : undefined
Dst-port        : undefined
Src-port        : undefined
Router-instance : management
Action          : permit
Log             : enabled
Matches         : 1424
=====

```

6.3 ACLs

ACL filter policies, also referred to as Access Control Lists (ACLs) or just “filters”, are sets of ordered rule entries specifying packet match criteria and actions performed on a packet after a match. Filter policies are created with a unique filter ID and filter name. After the filter policy is created, the policy must be associated with interfaces or services.

For more information about ACL configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

Example: Configuring and applying ACL filter policies

```

configure filter match-list port-list "AS7xx-Ports" { port 179 }
configure filter match-list port-list "AS7xx-Ports" range start 30000 end 64000 { }
configure filter ip-filter "AS700-ALLOW" filter-id 700
configure filter ip-filter "AS700-ALLOW" entry 10 { match protocol tcp }

```

```

configure filter ip-filter "AS700-ALLOW" entry 10 { match src-ip ip-prefix-list "SSH-Sources" }
configure filter ip-filter "AS700-ALLOW" entry 10 { match dst-ip ip-prefix-list "SNMP-Source" }
configure filter ip-filter "AS700-ALLOW" entry 10 { action accept }

configure filter ipv6-filter "AS-IPv6-ALLOW" filter-id 800
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 10 { match next-header tcp }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 10 { match src-ip ipv6-prefix-list "EBGP-v6-PEERS" }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 10 { match src-port port-list "AS7xx-Ports" }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 10 { action accept }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 20 { match next-header tcp }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 20 { match dst-ip ipv6-prefix-list "EBGP-v6-PEERS" }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 20 { match dst-port port-list "AS7xx-Ports" }
configure filter ipv6-filter "AS-IPv6-ALLOW" entry 20 { action accept }

configure router "Base" interface "To-Peering-LAN" ingress { filter ip "AS700-ALLOW" }
configure router "Base" interface "To-Peering-LAN" ingress { filter ipv6 "AS-IPv6-ALLOW" }

```

6.3.1 Rate limiting DDoS traffic

Use ACL policies to rate limit NTP, DNS, or other types of common DDoS packet types.

For more information about ACL configuration, see the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR Router Configuration Guide*.

Example: Rate limiting NTP and DNS packets

In the following example, rate limits are configured for NTP and DNS packets based on UDP, packet length, ports and destination IP.

```

configure filter match-list ip-prefix-list "Core-IP" { prefix 172.16.20.0/24 }
configure filter ip-filter "AS700-ALLOW" type packet-length
configure filter ip-filter "AS700-ALLOW" entry 20 { match protocol udp }
configure filter ip-filter "AS700-ALLOW" entry 20 { match dst-ip ip-prefix-list "Core-IP" }
configure filter ip-filter "AS700-ALLOW" entry 20 { match port eq 123 }
configure filter ip-filter "AS700-ALLOW" entry 20 { match packet-length gt 600 }
configure filter ip-filter "AS700-ALLOW" entry 20 { action accept }
configure filter ip-filter "AS700-ALLOW" entry 20 { action rate-limit pir 1000 }
configure filter ip-filter "AS700-ALLOW" entry 30 { match protocol udp }
configure filter ip-filter "AS700-ALLOW" entry 30 { match dst-ip ip-prefix-list "Core-IP" }
configure filter ip-filter "AS700-ALLOW" entry 30 { match port eq 53 }
configure filter ip-filter "AS700-ALLOW" entry 30 { match packet-length gt 600 }
configure filter ip-filter "AS700-ALLOW" entry 30 { action accept }
configure filter ip-filter "AS700-ALLOW" entry 30 { action rate-limit pir 1000 }

```

6.3.2 Redirecting suspicious traffic

Use ACL policies to redirect suspicious DDoS packets to a scrubbing device. This is achieved using Policy-Based Routing (PBR) and Policy-Based Forwarding (PBF) actions under the ACL context.

For more information about ACL configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

Example: Redirecting packets to a different next hop based on source or destination IP match

```
configure filter match-list ip-prefix-list "Core-IP" { prefix 172.16.20.0/24 }
configure filter ip-filter " pbr-nh-1 " filter-id 788
configure filter ip-filter "pbr-nh-1" entry 10 { match src-ip ip-prefix-list "Core-IP" }
configure filter ip-filter "pbr-nh-1" entry 10 { action forward next-hop nh-ip address
  172.19.20.3 }
configure filter ip-filter "pbr-nh-1" entry 20 { match dst-ip ip-prefix-list "Core-IP" }
configure filter ip-filter "pbr-nh-1" entry 20 { action forward next-hop nh-ip indirect
  true }
configure filter ip-filter "pbr-nh-1" entry 20 { action forward next-hop nh-ip address
  192.168.40.3 }
configure router "Base" interface "Interface-to-AS65501" ingress { filter ip "pbr-nh-1" }
```

6.3.3 ACL show commands

For more information about ACL configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

Use the following show commands to display IPv4 filter information.

```
show filter ip 10 associations
show filter ip 10 counters
show filter ip 10 detail
```

Use the following command to display all system resource usage information.

```
tools dump resource-usage system all | match 'ACL|Total'
```

6.4 PBR

SR OS-based routers support configuring of IPv4 and IPv6 redirect policies. Redirect policies allow a user to specify multiple redirect target destinations and define status check test methods to validate the ability for a destination to receive redirected traffic. For more information about Policy-Based Routing (PBR) configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

The following example displays a ping test used to verify the destination. If the destination is not reachable, traffic is not redirected to that destination, and regular route forwarding takes place.

Example: Configuring policy-based routing

```
configure filter redirect-policy "FIREWALL-V4" admin-state enable
configure filter redirect-policy "FIREWALL-V4" destination 10.200.200.0 { ping-test
  interval 5 }
configure filter redirect-policy "FIREWALL-V4" destination 10.200.200.0 { ping-test drop-
  count 1 }

configure filter ip-filter "ACL_PBR_V4" filter-id 155
configure filter ip-filter "ACL_PBR_V4" entry 1000 { match protocol ip }
```

```
configure filter ip-filter "ACL_PBR_V4" entry 1000 { action forward redirect-policy  
"FIREWALL-V4" }
```

7 Configuring QoS

SR OS implements Quality of Service (QoS) with a four-step process:

1. Classification
2. Queuing
3. Scheduling
4. Re-marking

For more information about QoS configuration, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*.

7.1 Classification

This following example displays packet classification using DSCP, EXP, protocol and destination IP address. The classification policy is then applied to the interface. For QoS on VPRN interfaces, similar configurations can be applied on the **sap-ingress** and **sap-egress** contexts within **configure qos**.

Example: Configuring QoS classification

```
configure qos match-list ip-prefix-list "Peering-Core" prefix 10.10.10.0/24
configure qos network "Peering-Ingress-QoS" policy-id 10
configure qos network "Peering-Ingress-QoS" ingress { dscp be fc be }
configure qos network "Peering-Ingress-QoS" ingress { dscp be profile out }
configure qos network "Peering-Ingress-QoS" ingress { lsp-exp 6 fc h1 }
configure qos network "Peering-Ingress-QoS" ingress { lsp-exp 6 profile in }
configure qos network "Peering-Ingress-QoS" ingress { ip-criteria entry 10 match protocol
tcp }
configure qos network "Peering-Ingress-QoS" ingress { ip-criteria entry 10 match dst-ip
ip-prefix-list "Peering-Core" }
configure qos network "Peering-Ingress-QoS" ingress { ip-criteria entry 10 action fc ef }

configure router "Base" interface "To-Peering-LAN" qos { network-policy "Peering-Ingress-
QoS" }
```

7.2 Queuing

The following example displays a sample configuration for the queuing step in the QoS packet flow. The queuing policy is applied to the FP context of the card.

Example: Configuring QoS queuing

```
configure qos network-queue "Peering-Queue" fc be { queue 1 }
configure qos network-queue "Peering-Queue" fc ef { queue 6 }
configure qos network-queue "Peering-Queue" fc h1 { queue 7 }
configure qos network-queue "Peering-Queue" fc nc { queue 8 }
configure qos network-queue "Peering-Queue" queue 1 { mbs 50.0 }
```

```

configure qos network-queue "Peering-Queue" queue 1 { rate pir 90 }
configure qos network-queue "Peering-Queue" queue 1 { rate cir 10 }
configure qos network-queue "Peering-Queue" queue 6 { cbs 70.0 }
configure qos network-queue "Peering-Queue" queue 6 { mbs 100.0 }
configure qos network-queue "Peering-Queue" queue 6 { rate pir 100 }
configure qos network-queue "Peering-Queue" queue 6 { rate cir 100 }
configure qos network-queue "Peering-Queue" queue 7 { rate pir 100 }
configure qos network-queue "Peering-Queue" queue 7 { rate cir 100 }
configure qos network-queue "Peering-Queue" queue 8 { rate pir 10 }
configure qos network-queue "Peering-Queue" queue 8 { rate cir 10 }

configure card 1 fp 1 { ingress network queue-policy "Peering-Queue" }

```

7.3 Scheduling

The following example displays a simple port-based scheduler that typically meets the requirements for a peering network. SR OS also supports hierarchical schedulers and slope policies.

After the scheduler policy is defined, it is applied to the physical port context.

Example: Configuring QoS scheduling

```

configure qos port-scheduler-policy "Peer-Scheduler" max-rate 100000000
configure qos port-scheduler-policy "Peer-Scheduler" level 1 { rate pir 90 }
configure qos port-scheduler-policy "Peer-Scheduler" level 1 { rate cir 10 }
configure qos port-scheduler-policy "Peer-Scheduler" level 6 { rate pir max }
configure qos port-scheduler-policy "Peer-Scheduler" level 6 { rate cir max }
configure qos port-scheduler-policy "Peer-Scheduler" level 7 { rate pir max }
configure qos port-scheduler-policy "Peer-Scheduler" level 7 { rate cir max }
configure qos port-scheduler-policy "Peer-Scheduler" level 8 { rate pir max }
configure qos port-scheduler-policy "Peer-Scheduler" level 8 { rate cir max }

configure port 1/1/c1/1 ethernet { egress port-scheduler-policy policy-name "Peer-
Scheduler" }

```

7.4 Re-marking

Re-marking configuration is done inside the same policy as the classification and is applied under the interface level as shown in the following example.

Example: Configuring QoS re-marking

```

configure qos network "Peering-Ingress-QoS" egress { fc be lsp-exp-in-profile 0 }
configure qos network "Peering-Ingress-QoS" egress { fc be lsp-exp-out-profile 0 }
configure qos network "Peering-Ingress-QoS" egress { fc ef dscp-in-profile af41 }
configure qos network "Peering-Ingress-QoS" egress { fc h1 lsp-exp-in-profile 6 }

configure router "Base" interface "To-Peering-LAN" qos { network-policy "Peering-Ingress-
QoS" }

```

8 Additional system configuration

The following sections describe optional system configurations.

8.1 Switching from the classic CLI to the MD-CLI

Before SR OS Release 23.3.R1, the default management configuration mode was classic CLI. The following configuration enables model-driven configuration mode, the MD-CLI, NETCONF and gRPC on the router.

Run the following command in the classic CLI, then log out and log in to enable the MD-CLI.

```
configure system management-interface configuration-mode model-driven
logout
```

Use the following commands to enable automatic configuration saves in model-driven interfaces, and to enable NETCONF and gRPC.

```
configure private
configure system { management-interface cli md-cli auto-config-save true }
configure system { management-interface netconf admin-state enable }
configure system { management-interface netconf auto-config-save true }
configure system { security user-params local-user user "user1" access netconf true }
configure system { grpc admin-state enable }
configure system { grpc allow-unsecure-connection }
configure system { grpc gnmi admin-state enable }
configure system { grpc gnmi auto-config-save true }
configure system { security user-params local-user user "user1" access grpc true }
commit
```

For more information about the MD-CLI, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI User Guide* and the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*.

8.2 User and profile management

SR OS supports local, TACACS+, RADIUS, or LDAP for authentication, authorization, and accounting (AAA).

Example: Configuring local management

```
configure system security aaa local-profiles profile "NOC-User" default-action deny-all
configure system security aaa local-profiles profile "NOC-User" entry 10 { match
  "configure system security" }
configure system security aaa local-profiles profile "NOC-User" entry 10 { action deny }
configure system security aaa local-profiles profile "NOC-User" entry 20 { match "show" }
configure system security aaa local-profiles profile "NOC-User" entry 20 { action permit }

configure system security user-params local-user user "markp" password "changeme"
```

```
configure system security user-params local-user user "markp" access { console true }
configure system security user-params local-user user "markp" console { member ["NOC-User"] }
```

For more information about AAA, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

8.3 NTP

The following example shows a Network Time Protocol (NTP) configuration.

Example: Configuring NTP

```
configure system { time ntp admin-state enable }
configure system { time ntp server 172.16.1.10 router-instance "Base" key-id 5 }
configure system { time ntp server 172.16.1.10 router-instance "Base" prefer true }
configure system { time ntp server 172.18.2.20 router-instance "Base" key-id 5 }
configure system { time ntp authentication-key 5 key "keyvalue" }
configure system { time ntp authentication-key 5 type message-digest }
```

8.4 System alarms and logging

SR OS has a default **log-id 99** for all events and **log-id 100** for events with severity major and higher.

User-defined logs can be created as shown in the following example. Log destination options are **file**, **memory**, **console**, **snmp**, **netconf**, or **syslog**.

For more information about logging, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

Example: Configuring user defined logs

```
show log log-id 99

show log log-id 100

configure log log-id "33" admin-state enable
configure log log-id "33" source { main true }
configure log log-id "33" source { security true }
configure log log-id "33" source { change true }
configure log log-id "33" destination { memory max-entries 500 }

configure log syslog "Syslog-server-1" address 192.168.15.190
configure log syslog "Syslog-server-1" port 514

configure log log-id "To-syslog" admin-state enable
configure log log-id "To-syslog" source { main true }
configure log log-id "To-syslog" source { security true }
configure log log-id "To-syslog" source { change true }
configure log log-id "To-syslog" destination { syslog "Syslog-server-1" }
```


9 Appendix A: Custom CLI commands (pySROS)

Custom Python applications can be written to run on SR OS. One example of an application is a custom CLI command. The following sample configuration shows how to configure a Python script `get_all_interfaces.py` to display all VPRN interfaces and the in/out packets in one output. For sample Python scripts, visit the Nokia pySROS [GitHub](#) repository.

For more information about pySROS, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* and the *pySROS API documentation*.

Example: Configuring a python script

```
configure python python-script "get_all_interfaces" { admin-state enable }
configure python python-script "get_all_interfaces" { urls ["cf3:\get_all_
interfaces.py"] }
configure python python-script "get_all_interfaces" { version python3 }

configure system management-interface cli md-cli environment command-alias { alias "all-
interfaces" }
configure system management-interface cli md-cli environment command-alias { alias "all-
interfaces" admin-state enable }
configure system management-interface cli md-cli environment command-alias { alias "all-
interfaces" description "show all VPRN interfaces" }
configure system management-interface cli md-cli environment command-alias { alias "all-
interfaces" python-script "get_all_interfaces" }
configure system management-interface cli md-cli environment command-alias { alias "all-
interfaces" mount-point "/"show" }
```

```
# show all-interfaces
=====
All Interfaces on all VPRNs
=====
=====
VPRN      Interface Name  IPv4 Address   Oper Status   Port:VLAN      In-Pkts
Out-Pkts
-----
100      VPRN100        99.99.99.75   up            loopback       0
0
150      To_Ixia        150.150.150.6 up            1/1/30:150    0
0
150      VPRN150        150.150.150.75 up            loopback       0
0
=====
=====
```

10 Appendix B: Configuration groups

SR OS supports the creation of configuration templates called configuration groups, which can be applied at different branches in the configuration using the **apply-groups** command as shown in the following example. To view the expanded configuration, use the **info inheritance** command under the branch context.

For more information about configuration groups, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI User Guide*.

Example: Creating a configuration group

```
configure groups group "Peer-isis" router "Base" isis 0 { interface "<Interface-to-AS.*>" }
configure groups group "Peer-isis" router "Base" isis 0 { interface "<Interface-to-AS.*>"
  hello-authentication-key "mykey" }
configure groups group "Peer-isis" router "Base" isis 0 { interface "<Interface-to-AS.*>"
  hello-authentication-type message-digest }
configure groups group "Peer-isis" router "Base" isis 0 { interface "<Interface-to-AS.*>"
  interface-type point-to-point }
configure groups group "Peer-isis" router "Base" isis 0 { interface "<Interface-to-AS.*>"
  level 2 metric 10 }

configure router "Base" { interface "Interface-to-AS65501" }
configure router "Base" isis 0 interface "Interface-to-AS65501" { apply-groups ["Peer-isis"] }

(pr)[/configure router "Base" isis 0 interface "Interface-to-AS65501"]
A:admin@sr101# info inheritance
  apply-groups ["Peer-isis"]
  ## inherited: from group "Peer-isis"
  hello-authentication-key "7NcYcNGWMxapfjrDQIyYNe1ZQ7HXjfy=" hash2
  ## inherited: from group "Peer-isis"
  hello-authentication-type message-digest
  ## inherited: from group "Peer-isis"
  interface-type point-to-point
  level 2 {
    ## inherited: from group "Peer-isis"
    metric 10
  }
}
```


Customer document and product support



Customer documentation

[Customer documentation welcome page](#)



Technical support

[Product support portal](#)



Documentation feedback

[Customer documentation feedback](#)