7705 Service Aggregation Router
Release 24.4.R1

Basic System Configuration Guide

Table of contents

List of tables

List of figures

1 Preface

This guide describes system concepts and provides configuration explanations and examples to configure the 7705 SAR boot options file (BOF) and perform system and file management functions.

This guide 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:** This manual generically covers Release 24.x content and may contain some content that will be released in later maintenance loads. Please see the 7705 SAR 24.x.Rx Software Release Notes, part number 3HE20411000xTQZZA, for information about features supported in each load of the Release 24.x software.

> **Note:** As of Release 23.4, software support for the following hardware has been deprecated:
> - 8-port Ethernet Adapter card, v2 (a8-ethv2) (3HE02776)
> - 12-port Serial Data Interface card, v1 (a12-sdi) (3HE03391)
> - 7705 SAR-W (3HE07349)
>
> These components are no longer recognized in the release.
>
> If information about any of the above components is required, please see the applicable installation guides in Release 22.10.

1.1 Audience

This guide is intended for network administrators who are responsible for configuring the 7705 SAR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Concepts described in this guide include the following:

- CLI concepts
- file system concepts
- boot options, configuration, image loading, and initialization procedures
- basic system management functions such as the system name, router location, and coordinates as well as network time protocols and synchronization properties

1.2 Technical support

If you purchased a service agreement for your 7705 SAR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased a Nokia service agreement, follow this link to contact a Nokia support representative and to access product manuals and documentation updates:

Product Support Portal

2 7705 SAR system configuration process

The following table lists the tasks that are required to navigate the Command Line Interface (CLI), configure basic router and system parameters, perform operational functions with directory and file management, and configure boot option parameters.

Each chapter in this book is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

Area	Task/Description	Chapter
CLI Usage	Navigate the CLI and perform basic configuration tasks	CLI usage
Operational functions	Perform general operational functions for directory and file management	File system management
Boot options	Configure the boot options file (BOF)	Boot options
System configuration	Configure system functions, including host name, address, domain name, and time parameters	System management
Reference	List of security and telecom standards, supported protocols, and proprietary MIBs	Supported standards and protocols

3 CLI usage

This chapter provides information about using the Command Line Interface (CLI).

Topics in this chapter include:

- CLI structure
- Navigating in the CLI
- Getting help in the CLI
- The CLI command prompt
- Displaying configuration contexts
- EXEC files
- CLI script control
- Entering CLI commands
- CLI configuration rollback
- Transactional configuration
- Basic command reference

3.1 CLI structure

The 7705 SAR CLI is a command-driven interface accessible through the console, or through Telnet, secure shell (SSH), or SSH file transfer protocol (SFTP). The CLI can be used for configuration and management of 7705 SAR routers.

The 7705 SAR CLI command tree is a hierarchical inverted tree. The highest level is the root level. Below this level are other tree levels for the major command groups; for example, **configure** commands and **show** commands are below the root level.

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

Figure 1: Root-Level Commands displays the major contexts for router configuration. The figure is a sample representation of high-level commands; not all commands are included.

Figure 1: Root-Level Commands

ROOT
ADMIN —— debug-save
                                                                                    disconnect
                                                                                    display-config
BOF ——— address   enable-tech
                                                              autonegotiate   reboot
                                                              console-speed   redundancy
CLEAR ————————————————————————————————————— card   dns-domain   save
                                             cron   duplex   set-time
                                             filter   persist   tech-support
CONFIGURE ————————————————————— card   log   primary-config
                                cron   mda   primary-dns
                                eth-cfm   port   primary-image
                                filter   router   save
DEBUG ——————————— oam   log   saa   secondary-config
                  ppp   port   screen   secondary-dns
                  radius   qos   service   secondary-image
ENVIRONMENT ——— alias   router   redundancy   system   speed
                create   service   router   tacplus   static-route
                more   snmp   saa   tertiary-config
                reduced-prompt sync-if-timing service   tertiary-dns
                saved-ind-prom system   system   tertiary-image
                terminal   wait
                time-display
                time-stamp

FILE —— attrib
                                                              cd
                                                              copy
HELP —— help   delete
                                               help edit   dir
                                               help globals   format
MONITOR ————————————————————— filter   md
                              management-access-filter   move
                              port   rd
PASSWORD   router   repair
                              service   scp
                                                              shutdown
SHOW ————————————— alias   type
                   bof   version
                   boot-messages
TOOLS ——— dump   card
          perform chassis
                   cron
                   debug
                   eth-cfm
                   filter
                   log
                   mda
                   multilink-bundle
                   pools
                   port
                   qos
                   redundancy
                   router
                   saa
                   service
                   snmp
                   system
                   time
                   uptime
                   users
                   version

21699

3.2 Navigating in the CLI

The following sections describe additional navigational and syntax information:

- CLI contexts
- CLI syntax
- CLI root-level commands
- CLI global commands
- CLI environment commands
- CLI monitor commands

3.2.1 CLI contexts

The CLI is used to access, configure, and manage 7705 SAR routers. CLI commands are entered at the command line prompt. Access to specific CLI commands is controlled by the permissions set by the system administrator. Entering a CLI command makes navigation possible from one command context (or level) to another. When the user enters a CLI session, they are in the root context. To navigate to other levels, the user enters the name of successively lower contexts. For example, entering the **configure** or **config** command at the root level takes the user to the **config** context. The active CSM slot displays in the command prompt at the beginning of the CLI context as shown below:

```
A:NOK-12# config
    A:NOK-12>config#
```

In any CLI context, commands can be entered at that context level by entering the text. Pressing <Enter> moves to a lower context. The user can also include commands from lower contexts at one context level as long as the command and parameter syntax is correct.

The following example shows two methods of navigating to a service SDP ingress level:

Method 1: Enter all commands on a single line.

```
    A:NOK-12# configure service cpipe 6 spoke-sdp 2:6 ingress
    *A:NOK-12>config>service>cpipe>spoke-sdp>ingress#
```

Method 2: Enter each command on a separate line.

```
    A:NOK-12>config# service
    A:NOK-12>config>service# cpipe 6
    *A:NOK-12>config>service>cpipe# spoke-sdp 2:6
    *A:NOK-12>config>service>cpipe>spoke-sdp# ingress
    *A:NOK-12>config>service>cpipe>spoke-sdp>ingress#
```

The CLI returns an error message if the syntax is incorrect.

```
    A:NOK-12>config>service# cpipe6
    Error: Bad command.
```

3.2.2 CLI syntax

Table 2: Command Syntax Symbols lists command syntax symbols. Differences between the syntax used in the CLI and in the Command Reference sections of the 7705 SAR guides is noted in the table.

Table 2: Command Syntax Symbols

Symbol	Description	Example
|	A vertical bar represents an OR, indicating that only one of the parameters in the brackets or braces can be selected	**tcp-ack {true | false}**
[ ]	Brackets indicate optional parameters	**router** [**router-name**]
< >	Angle brackets indicate that the user must enter a value for the parameter inside the brackets (Note: angle brackets are not used in the 7705 SAR guides but are used on the CLI; italics are used in these guides to indicate the same rule)	**interface** *<interface-name>*
{ }	Braces indicate that one of the parameters must be selected	**default-action {drop | forward}**
[{ }]	Braces within square brackets indicate that the parameters are optional, but if one is selected, the information in the braces is required; for example, if the user selects the **peer** parameter, they must enter the keyword **peer** (*ip-address* is optional)	**discovery** [{**peer** [*ip-address*]} | {**interface** [*ip-int-name*]}]
Bold	In the 7705 SAR guides (not on the CLI), bold indicates commands and keywords that the user must enter exactly as shown	**scope {inclusive | template}**
Italic	In the 7705 SAR guides (not on the CLI), italics indicate parameters that the user must enter a value for	*dscp dscp-name*
n/a	In the Command Reference section, n/a in the Default field of a command indicates that a default value is not applicable for the command	—

3.2.3 CLI root-level commands

The commands listed in Table 3: Operational root commands are available at the root level of the CLI hierarchy. For the command descriptions, see the Command Reference sections of the applicable guides.

Table 3: Operational root commands

Command	Description
admin	Enters the administrative context for system operations
bof	Enters the context to configure the boot options file
clear	Clears statistics or resets the operational state
configure	Enters the configuration context
[**no**] **debug**	Enters the context to enable or disable debugging and specify debug options
environment	Enters the environment configuration context
file	Enters the context for file system commands
help	Displays help in the CLI
monitor	Enters the context to monitor statistics
password	Enters the context to change the user CLI login password
show	Shows operational information
tools	Enters the tools context for troubleshooting and debugging

3.2.4 CLI global commands

The commands listed in Table 4: CLI global commands are implemented as global commands that can be entered at any level in the CLI hierarchy. The exception is the **info** command, which can only be entered in a configuration context. To display a list of all system global commands, enter **help globals** in the CLI.

Table 4: CLI global commands

Command	Description
back	Navigates the user to the parent context
candidate	Enters the context to configure candidate parameters
echo	Echoes the text that is typed in; its primary use is to display messages to the screen within an exec file
enable-admin	Enables the user to become a system administrator
exec	Executes the contents of a text file as if they were CLI commands entered at the console
exit	Returns the user to the previous higher context

Command	Description
exit all	Returns the user to the root context
help	Displays help in the CLI
history	Displays a list of the most recently entered commands
info	Displays the running configuration for a configuration context; is not supported at the top (**config**) level
logout	Terminates the CLI session
mrinfo	Displays multicast information from the target multicast router. See the 7705 SAR OAM and Diagnostics Guide for details.
mstat	Traces a multicast path from a source to a receiver and displays multicast packet rate and loss information. See the 7705 SAR OAM and Diagnostics Guide for details.
mtrace	Traces a multicast path from a source to a receiver and displays hop-by-hop information. See the 7705 SAR OAM and Diagnostics Guide for details.
oam	Provides OAM test suite options. See the 7705 SAR OAM and Diagnostics Guide for details.
ping	Verifies the reachability of a remote host
pwc	Displays the present or previous working context of the CLI session
sleep	Causes the console session to pause operation (sleep) for 1 s or for the specified number of seconds; its primary use is to introduce a pause within the execution of an exec file
ssh	Opens a secure shell connection to a host
telnet	Telnets to a host
traceroute	Determines the route to a destination address
tree	Displays a list of all commands at the current level and all sublevels
write	Sends a console message to a specific user or to all users with active console sessions

3.2.5 CLI environment commands

The CLI **environment** commands listed in Table 5: CLI environment commands are found in the **root>environment** context of the CLI tree. These commands control session preferences for a single CLI session.

Table 5: CLI environment commands

Command	Description
alias	Enables the substitution of a command line by an alias
create	Enables or disables the use of a create parameter check
kernel	Enables or disables the kernel; the command is enabled with the enable-tech command
more	Enables the CLI output to be displayed one screen at a time, awaiting user input to continue
reduced-prompt	Configures the maximum number of higher-level CLI context nodes to display by name in the CLI prompt for the current CLI session
saved-ind-prompt	Saves the indicator in the prompt
shell	Enables or disables the shell; the command is enabled with the **enable-tech** command
suggest-internal-objects	Enables the suggestion of internally created objects while auto-completing
terminal	Configures the terminal screen length for the current CLI session
time-display	Specifies whether time should be displayed in local time or UTC
time-stamp	Specifies whether a timestamp should be displayed before the prompt

3.2.6 CLI monitor commands

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

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

The **<Ctrl-c>** keystroke interrupts a monitoring process. Monitor command configurations cannot be saved. The commands must be entered for each monitoring session. If the maximum limits are configured, the statistical information can be monitored for a maximum of 60 × 999 s (approximately 1000 minutes, or 16.6 hours).

The CLI monitor commands are listed in Table 6: CLI monitor commands . For the command descriptions, see the Command Reference sections of the applicable guides.

Table 6: CLI monitor commands

Command	Description
cpm-filter	Monitors commands for CPM filters
fabric-profile	Monitors fabric traffic statistics
filter	Enables IP and MAC filter monitoring at a configurable interval until that count is reached
lag	Monitors traffic statistics for LAG ports
management-access-filter	Monitors commands for management access filters
port	Enables port traffic monitoring. The statistical information for the specified ports displays at the configured interval until the configured count is reached.
router	Enables virtual router instance monitoring at a configurable interval until that count is reached
scada	Monitors SCADA traffic statistics
service	Monitors commands for a particular service

3.3 Getting help in the CLI

The **help** system commands and the **?** key display different types of help in the CLI. Table 7: Online help commands lists the help commands.

Table 7: Online help commands

Command	Description
help	Displays instructions for getting CLI help
?	Lists all commands in the current context
command **?**	Displays the command's syntax and associated keywords
command keyword **?**	Lists the associated arguments for *keyword* in *command*
string\<Tab\> *string\<space\>*	Completes a partial command name (auto-completion) or lists available commands that match *string*

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

The **tree flat** command displays the command hierarchy on single lines; for example:

```
card
card card-type
card mda
card mda access
card mda access ingress
card mda access ingress fabric-policy
card mda access ingress security-queue-policy
card mda ais-propagation
card mda clock-mode
```

Figure 2: CLI Display for CLI Tree Help shows a partial list of the outputs of the **tree** and **tree detail** commands entered at the **config** level.

Figure 2: CLI Display for CLI Tree Help

```
*A:ALU-12>config# tree                          *A:ALU-12>config# tree detail
configure                                       configure
+---card                                         +---card <slot-number>
|   +---card-type                                |   no card <slot-number>
|   +---mda                                      |   +---card-type <card-type>
|   |   +---clock-mode                           |   |   no card-type
|   |   +---mda-type                             |   +---mda <mda-slot>
|   |   +---network                              |   |   no mda <mda-slot>
|   |   |   +---ingress                          |   |   +---clock-mode adaptive
|   |   |   |   +---queue-policy                 |   |   +---mda-type <mda-type>
|   |   +---shutdown                             |   |   |   no mda-type
|   +---shutdown                                 |   |   +---network
+---cron                                         |   |   |   +---ingress
|   +---action                                   |   |   |   |   +---no queue-policy
|   |   +---expire-time                          |   |   |   |   |   queue-policy <name>
|   |   +---lifetime                             |   |   +---no shutdown
|   |   +---max-completed                        |   |   |   shutdown
|   |   +---results                              |   +---no shutdown
|   |   +---script                               |   |   shutdown
|   |   +---shutdown                             +---cron
|   +---schedule                                 |   +---action <action-name> [owner <action-owner>]
|   |   +---action                               |   |   no action <action-name> [owner <action-owner>]
|   |   +---count                                |   |   +---expire-time {<seconds>|forever}
|   |   +---day-of-month                         |   |   +---lifetime {<seconds>|forever}
|   |   +---description                          |   |   +---max-completed <unsigned>
|   |   +---end-time                             |   |   +---no results
|   |   +---hour                                 |   |   |   results <file-url>
|   |   +---interval                             |   |   +---no script
|   |   +---minute                               |   |   |   script <script-name> [owner <script-owner>]
|   |   +---month                                |   |   +---no shutdown
|   |   +---shutdown                             |   |   |   shutdown
|   |   +---type                                 |   +---no schedule <schedule-name> [owner <schedule-owner>]
|   |   +---weekday                              |   |   schedule <schedule-name> [owner <schedule-owner>]
|   +---script                                   |   |   +---action <action-name> [owner <action-owner>]
|   |   +---description                          |   |   |   no action
|   |   +---location                             |   |   +---count <number>
|   |   +---shutdown                             |   |   |   no count
+---filter                                       |   |   +---day-of-month {<day-number> [..<day-number>]|all}
|   +---ip-filter                                |   |   |   no day-of-month
|   |   +---default-action                       |   |   +---description <description-string>
|   |   +---description                          |   |   |   no description
|   |   +---entry                                |   |   +---end-time [<date>|<day-name>] <time>
|   |   |   +---action                           |   |   |   no end-time
|   |   |   +---description                      |   |   +---hour {<hour-number> [..<hour-number>]|all}
|   |   |   +---match                            |   |   |   no hour
|   |   |   |   +---dst-ip                       |   |   +---interval <seconds>
|   |   |   |   +---dst-port                     |   |   |   no interval
|   |   |   |   +---icmp-code                    |   |   +---minute {<minute-number> [..<minute-number>]|all}
|   |   |   |   +---icmp-type                    |   |   |   no minute
|   |   |   |   +---src-ip
|   |   |   |   +---src-port
|   |   +---renum
|   |   +---scope                                                                              21701
```

3.4 The CLI command prompt

By default, the CLI command prompt indicates the device being accessed, the active CSM, and the current CLI context. For example, the prompt **A:NOK-1>config> router#** indicates that the active CSM is CSM A, the user is on the device with hostname **NOK-1**, and the current context is **configure router**. In the prompt, the separator used between contexts is the "**>**" symbol.

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

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

All special characters (#, $, and so on) must be enclosed within double quotes; otherwise, the character is seen as a comment character and all characters on the command line following the "#" are ignored. For example:

```
*A:NOK-1>config>router>mpls# authentication-key "router#1"
```

This example shows a security configuration over a network link. Because the string "router#1" is enclosed within double quotes, it is recognized as a password for the link.

When changes are made to the configuration file, a "*" appears in the prompt string (***A:NOK-1**), indicating that the changes have not been saved. When an admin **save** command is executed, the "*" disappears. This behavior is controlled by the **saved-ind-prompt** command in the **environment** context.

3.5 Displaying configuration contexts

The **info**, **info detail**, and **info operational** commands display the configuration for the current level. The **info** command displays non-default configurations. The **info detail** command displays the entire configuration for the current level, including defaults. The **info operational** command is used to display the operational configuration of the current configuration context when the user is in candidate edit mode.

The following example shows the output that displays using the **info** command and the output that displays using the **info detail** command.

```
*A:NOK-1>config>router# interface system
*A:NOK-1>config>router>if# info
----------------------------------------------
            address 10.221.221.72/8
----------------------------------------------
*A:NOK-1>config>router>if#
```

```
*A:NOK-1>config>router>if# info detail
----------------------------------------------
            address 10.221.221.72/8
            no description
            no arp-timeout
            icmp
                mask-reply
                unreachables 100 10
                ttl-expired 100 10
            exit
```

```
            no ntp-broadcast
            no shutdown
            no bfd
----------------------------------------------
*A:NOK-1>config>router>if#
```

The **info** commands can be used in every configuration context except for the top (**config**) level.

3.6 EXEC files

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

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

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

3.7 CLI script control

The 7705 SAR provides centralized script management for CLI scripts that are used by CRON and the event handling system (EHS). Scripts contain a set of CLI commands that are executed at a scheduled time or when an event is triggered. A set of script policies and script objects can be configured to control such things as:

- where scripts are located (local compact flash or remote FTP server)

- where the output of the results is stored

- how long historical script result records are kept

- how long a script may run

Script parameters are configured under the **config>system>script-control** context.

A script is assigned a script name and optional owner. The owner is an arbitrary string; it is not associated with an actual CLI user. Multiple owners can be associated with a script name, and each script name/ owner combination is unique.

A script is also associated with a script text filename and its location. The text file contains the CLI commands to be executed.

When a script has been defined, a script policy is configured under the **config>system>script-control** context and associated with the script. A script policy is assigned a policy name and optional owner. The owner is an arbitrary string; it is not associated with an actual CLI user. Multiple owners can be associated with a script policy name, and each script policy name/owner combination is unique.

The script policies are referenced by the CRON scheduler and the EHS event handler. All configured script policies can be used by both CRON and EHS.

The script text files can be stored on the local compact flash or on a remote FTP/TFTP server. In CSM-redundant 7705 SAR-8 Shelf V2 or 7705 SAR-18 systems, the script text files must be saved in the compact flash of both CSMs so that CRON or EHS configurations are not lost if a CSM switchover

occurs. However, a CSM switchover does cause all queued scripts to be dropped. For remote servers, communication must be reliable; otherwise, there may be undesired pauses during script execution.

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

For information about CRON, see CRON in this guide. For information about the EHS, see the 7705 SAR System Management Guide, "Event handling system".

3.8 Entering CLI commands

The following sections describe more information about entering CLI commands:

- Command completion
- Unordered parameters
- Editing keystrokes
- Absolute paths
- History
- Entering numerical ranges or lists
- Pipe/match
- Pipe/count
- Redirection

3.8.1 Command completion

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

The command completion functionality works for both keywords and for optional parameters that have already been configured. When using command completion for optional parameters, **Tab** must be used.

For example, entering "i <Tab> returns the following user-configured interface names:

```
*A:NOK-12>config>router# interface "i
"igmp_interface"    "igmp_interface2"   "isis_interface"
```

System commands are available at all CLI context levels.

3.8.2 Unordered parameters

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

3.8.3 Editing keystrokes

When entering a command, special keystrokes allow for editing of the command. Table 8: Command editing keystrokes lists the command editing keystrokes.

Table 8: Command editing keystrokes

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

3.8.4 Absolute paths

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

```
*A:NOK-12# configure router
*A:NOK-12>config>router# interface system address 192.0.2.0
*A:NOK-12>config>router# /admin save
A:NOK-12>config>router# \clear router bfd session all
A:NOK-12>config>router#
```

The command may or may not change the current context depending on whether it is a leaf command. This is the same behavior the CLI performs when CLI commands are entered individually; for example:

```
*A:NOK-12# admin
*A:NOK-12>admin# save
```

or

```
*A:NOK-12# admin save
*A:NOK-12#
```

3.8.5 History

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

```
*A:NOK-1# history
     1 environment terminal length 48
     2 show version
     3 configure port 1/1/1
     4 info
     5 show port 1/1/1
     6 \con port 1/1/1
     7 \configure router mpls
     8 info
     9 \configure system login-control
    10 info
    11 history
*A:NOK-1# !2
*A:NOK-1# show version
TiMOS-B-0.0.I322 both/hops NOKIA SAR 7705
Copyright (c) 2018 Nokia.All rights reserved.
All use subject to applicable license agreements.
Built on Wed Jan 17 01:05:13 EST 2018 by csabuild in /re8.0/I322/panos/main
*A:NOK-1#
```

3.8.6 Entering numerical ranges or lists

The 7705 SAR CLI allows the use of a single numerical range, a list of values (elements), or a combination of both as an argument in the command line.

A range in a CLI command is limited to positive integers and is denoted with two numbers enclosed in square brackets with two periods (".."") between the numbers [x.. y], where *x* and *y* are positive integers and *y-x* is less than 1000. For example, to configure a range of VPLS service IDs from 20 to 30 for a customer, enter:

config service vpls [20..30] customer 1 create no shutdown

A list of values contains discrete integer elements, in any order. For example, to configure a list of VPLS service IDs that are not sequential, enter:

config service vpls [3,5,7] customer 1 create no shutdown

To configure a list of interface names (interface names must begin with a letter), put the alphabetic part of the name outside of the brackets; for example:

config router interface intf[1,4,6] no shutdown

This command creates interfaces with names intf1, intf4, and intf6.

Lists can contain ranges as elements, as well as values. For example, to configure multiple ports on MDA 1, enter:

config port 1/1[1..6,8,10, 21..32] no shutdown

CLI commands can also contain ranges or lists of hexadecimal values; for example, [0x0f..0x13], [0x4,0x8,0xc]. This allows ranges to be used when working with data that is normally expressed in hexadecimal, such as IPv6 addresses or MAC addresses.

A range can also be a reference to a previous range in the same command. This reference takes the form [$*x*], where *x* is an integer between 0 and 5, with 0 referring to the first range in the command, 1 to the second, and so on up to the maximum of six ranges. For example:

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

gives vprn 11 the router ID 10.20.11.1, vprn 12 the router ID 10.20.12.1, and so on.

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

Specifying a range in the CLI does have limitations. These limitations are summarized in Table 9: CLI range use limitations .

Table 9: CLI range use limitations

Limitation	Description/example
Up to six ranges (including references) can be specified in a single command but must not combine to more than 1000 iterations of the command	For example, ports on two adapter cards can be shut down in one command by using two ranges: **config port 1/[1..2]/[1..10] shutdown** This command shuts down ports 1 to 10 on MDA 1 and MDA 2.
Ranges within quotation marks are interpreted literally	Enclosing a string in quotation marks ("*string*") causes the string to be treated literally and as a single parameter. For example, several commands in the 7705 SAR CLI allow the configuration of a descriptive string. If the string is more than one word and includes spaces, it must be enclosed in quotation marks. A range that is enclosed in quotes is also treated literally. For example, **config router interface "A[1..10]" no shutdown**

Limitation	Description/example
	creates a single router interface with the name "A[1..10]". However, a command such as: **config router interface A[1..10] no shutdown** creates 10 interfaces with names A1, A2, to A10.
The range cannot cause a change in contexts	Commands should be formed in such a way that there is no context change upon command completion. For example, **config port 1/1/[1..10]** attempts to change 10 different contexts. When a range is specified in the CLI, the commands are executed in a loop. On the first loop execution, the command changes contexts, but the new context is no longer valid for the second iteration of the range loop. A "Bad Command" error is reported and the command aborts. Adding **shutdown** or **no shutdown** to the command keeps the same context.
Command completion may not work when entering a range	After entering a range in a CLI command, command and key completion, which normally occurs by pressing the <Tab> key or spacebar, may not work. If the command line entered is correct and unambiguous, the command works properly; otherwise, an error is returned.

3.8.7 Pipe/match

The 7705 SAR supports the pipe/match (...| **match**) feature to search one or more files for a specified character string or pattern.

Match syntax:

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

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

where:

pattern: a string or regular expression (maximum 200 characters)

context: displays the context associated with the matching line

parents: displays the parent context information

children: displays the child context information

all: displays both parent and child context information

ignore-case: ignores the case in the string (uppercase or lowercase)

max-count *lines-count*: displays the matching lines, up to the specified number (1 to 2147483647)

expression: the pattern is interpreted as a regular expression

invert-match: displays all the lines that do not contain the string specified in *pattern*

pre-lines *pre-lines*: displays the lines before the matching line, up to the specified number (0 to 100)

post-lines *lines-count*: displays the lines after the matching line, up to the specified number (1 to 2147483647)

For example:

```
*A:NOK-12# show service sap-using | match 1/1 pre-lines 10
===============================================================================
Service Access Points
===============================================================================
PortId                     SvcId      Ing.  Ing.   Egr.  Egr.   Adm  Opr
                                      QoS   Fltr   QoS   Fltr
-------------------------------------------------------------------------------
1/1/1:333                  111        1     none   1     none   Up   Up
1/1/1:444                  111        1     none   1     none   Up   Up
1/1/9:10                   200        1     none   1     none   Up   Up
1/1/9:11                   200        1     none   1     none   Up   Up
1/1/9:12                   200        1     none   1     none   Up   Up
1/1/9:13                   200        1     none   1     none   Up   Up
1/1/9:14                   200        1     none   1     none   Up   Up
1/1/9:15                   200        1     none   1     none   Up   Up
```

```
A:NOK-12# show log log-id 98 | match ignore-case "sdp bind"
"Status of SDP Bind 101:1002 in service 1001 (customer 1)changed to admin=up oper=up
flags="
"Processing of a SDP state change event is finished and status of all affected SDP
Bindings on SDP 101 has been updated."

A:NOK-12# show log log-id 98 | match max-count 1 "service 1001"
"Status of service 1001 (customer 1)changed to administrative state: up, operational
state: up"

*A:NOK-12# admin display-config | match post-lines 5 max-count 2 expression "snmp"

        snmp
        exit
        login-control
            idle-timeout disable
            pre-login-message "csasim2 - " name
        exit
            snmp
                view "testview" subtree "1"
                    mask ff
                exit
                view "testview" subtree "1.3.6.1.2"
                    mask ff type excluded
*A:NOK-12#
```

Table 10: Pipe/match characters describes regular expression symbols and interpretation (similar to what is used for route policy regexp matching).

Table 10: Pipe/match characters

String	Description
.	Matches any single character

String	Description
[ ]	Matches a single character with what is contained within the brackets [abc] matches "a", "b", or "c" [a-z] matches any lowercase letter [A-Z] matches any uppercase letter [0-9] matches any number
[^]	Matches a single character with what is not contained within the brackets [^abc] matches any character other than "a", "b", or "c" [^a-z] matches any single character that is not a lowercase letter
^	Matches the start of the line (or any line, when applied in multiline mode)
$	Matches the end of the line (or any line, when applied in multiline mode)
()	Defines a "marked subexpression" Every matched instance is available to the next command as a variable
*	A single character expression followed by "*" matches zero or more copies of the expression
{m,n}	Matches at least m and at most n repetitions of the term
{m}	Matches exactly m repetitions of the term
{m,}	Matches m or more repetitions of the term
?	The preceding item is optional and matched at most once
+	The preceding item is matched one or more times
-	Used between start and end of a range
\	An escape character to indicate that the following character is a match criterion and not a grouping delimiter

Table 11: Special characters identifies the special character options.

Table 11: Special characters

Options	Similar to	Description
[:upper:]	[A-Z]	Uppercase letters
[:lower:]	[a-z]	Lowercase letters
[:alpha:]	[A-Za-z]	Uppercase and lowercase letters
\w	[A-Za-z_]	Word characters

Options	Similar to	Description
[:alnum:]	[A-Za-z0-9]	Digits, uppercase and lowercase letters
[:digit:]	[0-9]	Digits
\d	[0-9]	Digits
[:xdigit:]	[0-9A-Fa-f]	Hexadecimal digits
[:punct:]	[.,!?:...]	Punctuation
[:blank:]	[\t]	Space and Tab
[:space:]	[\t\n\r\f\v]	Blank characters
\s	[\t\n\r\f\v]	Blank characters

3.8.8 Pipe/count

The 7705 SAR supports a pipe/count command (...| **count**) that provides a count of the number of lines that would have otherwise been displayed. The pipe/**count** command is particularly useful when used in conjunction with the pipe/**match** command to count the number of output lines that match a specified pattern.

For example:

```
*A:NOK-12# show service service-using vprn
===============================================================================
Services [vprn]
===============================================================================
ServiceId  Type       Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
1          VPRN       Down Down 1
44         VPRN       Up   Up   1
100        VPRN       Down Down 1
102        VPRN       Up   Up   1
235        VPRN       Down Down 1
1000       VPRN       Down Down 1000
-------------------------------------------------------------------------------
Matching Services : 6
-------------------------------------------------------------------------------
===============================================================================
*A:NOK-12# show service service-using vprn | match Down | count
Count: 4 lines
*A:NOK-12#
```

3.8.9 Redirection

The 7705 SAR supports redirection (>), which allows the operator to store the output of a CLI command as a local or remote file.

```
'ping <customer_ip> > cf3:/ping/result.txt'
'ping <customer_ip> > ftp://ron@ftp.alcatel.com/ping/result.txt'
```

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

```
ping 10.0.0.1 | match expression "time.\d+" > cf3:/ping/time.txt
```

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

3.9 CLI configuration rollback

The CLI configuration rollback feature allows operators to save rollback checkpoint and rescue files that can be used to quickly return the node configuration to a previous state with minimal impacts to services and without restarting the node.

CLI configuration rollback gives operators better control and visibility over router configurations and reduces operational risk while increasing flexibility and providing powerful recovery options.

The location and generic filename of the rollback checkpoint and rescue files must be configured with the **rollback-location** and **rescue-location** commands before a rollback file can be saved. Files can be saved locally on the compact flash or on a remote device. The file URL must contain a path or directory and a generic filename with no extension. File suffixes are automatically appended when the file is saved.

3.9.1 Rollback checkpoint and rescue files

Rollback checkpoint files and rescue files are created with the rollback **save** command. A rollback checkpoint file can be saved at any time or configured to be automatically saved on a recurring schedule using the 7705 SAR CRON feature. For more information, see CRON.

Rollback checkpoint and rescue files contain all current operationally active configurations, including configuration changes from CLI commands in the config context and SNMP sets. Rollback checkpoint files are intended to be saved whenever there have been a moderate number of changes to the configuration, in order to create a series of intermediate checkpoints that operators can return to. The rollback rescue file is intended to be a permanent stable configuration that can be reverted to if needed.

Rollback checkpoint and rescue files do not contain any BOF configuration information or any configuration or state changes performed under the debug branch of the CLI. Similarly, performing a CLI configuration rollback never impacts the BOF configuration or any command from the debug CLI branch.

When a rollback **save** command is executed, a rollback checkpoint or rescue file is saved in the configured location. The latest rollback checkpoint file is saved with the suffix *.rb. The suffixes of all previously saved rollback checkpoint files are automatically incremented by one (*.rb becomes *.rb.1, *.rb.1 becomes *.rb.2, and so on). The rescue file is saved with the suffix *.rc.

By default, there can be 10 rollback checkpoint files, the latest with suffix *.rb and nine older files with suffixes *.rb.1 through *.rb.9. If the maximum number of checkpoint files is reached and a new one is saved, the oldest checkpoint file is deleted. The maximum number of rollback checkpoint files that can be saved can be configured with the **local-max-checkpoints** and **remote-max-checkpoints** commands.

There can only be one rollback rescue file. When a new rescue file is saved, the existing file is deleted. The rescue file is not impacted by the number of rollback checkpoint files — there will always be one rescue file available.

Operators can view a list of rollback checkpoint or rescue files with the rollback **view** command. The following information is displayed for the files:

- date and time stamps

- file index and suffix

- the user who created the file

- release number

- comment string

A rollback **compare** command is also available that allows operators to compare different checkpoint files to each other or to the current operating configuration. The command output highlights any differences between the configurations.

Rollback checkpoint and rescue files are not editable or interchangeable with configuration files, such as those generated with an **admin save** command.

Both **admin save** and **rollback save** should be performed periodically. The **admin save** command backs up the complete configuration file to be used during a router reboot and should be performed after any major service changes or hardware and software upgrades. The **rollback save** command should be performed to create intermediate checkpoints whenever a moderate number of changes have been made to the configuration.

Rollback checkpoint files and rescue files can be deleted with the dedicated **admin**>**rollback**>**delete** command. When a checkpoint file is deleted, the suffix ID numbers of all older files are automatically decremented.

If a rollback checkpoint file is manually deleted, using, for example, the **file delete** command, the suffix ID numbers of older checkpoint files are not decremented, nor is the backup checkpoint file deleted from the standby CSM. This creates a gap in the checkpoint file list. New rollback checkpoint files can still be created, but the gap is not filled until enough files have been created to roll the gap off the end of the list.

3.9.1.1 Rollback file backup

The rollback checkpoint files can be backed up from the active CSM to the standby CSM on the 7705 SAR-8 Shelf V2 or 7705 SAR-18 with the **rollback-sync** command in the **admin** context. Rollback file backups are not supported on fixed platforms because they do not have redundant CSMs.

The 7705 SAR also supports automatic synchronization with the **rollback-sync** command in the **config** context. When automatic rollback synchronization is enabled, a rollback **save** causes the new checkpoint file to be saved on both the active and standby CSMs if the rollback location is a local location. The suffixes of all older checkpoint files on both active and standby CSMs are incremented by one. Automatic synchronization only causes newly created rollback checkpoint files to be copied to both CSMs. Any rollback checkpoint files that were created before automatic synchronization was enabled are not copied to the standby CSM but can be manually backed up with the **rollback-sync** command in the **admin** context.

If the **config**>**rollback-sync** command is enabled, deleting a rollback checkpoint file also deletes the backup file and decrements the suffix ID numbers on the standby CSM.

The dedicated **rollback-sync** commands are the only commands that can be used to back up rollback checkpoint files. Existing redundancy synchronization commands are not compatible with rollback checkpoint files.

3.9.2 Performing a CLI configuration reversion

The rollback **revert** command is used to return the CLI configuration, including all configuration commands and SNMP sets, to the saved configuration in a rollback checkpoint or rescue file. CLI configuration reversion can be used to quickly correct problems in the configuration during network operation or to aid in experimentation by enabling a return to known settings after trying a new configuration.

The CLI configuration reversion is performed without a reboot and with minimal impact on the services being provided by the 7705 SAR. Configuration parameters that have changed since the checkpoint file was created, or items on which changed configurations have dependencies, are first reset to their default values and then restored to their previous values from the rollback checkpoint file. Performing a configuration reversion can be briefly service-impacting in changed areas. There are no service impacts to configuration areas that did not change since the rollback checkpoint file was created.

If a rollback reversion process includes any commands that will remove, rebuild, or reboot an adapter card or fixed platform, the impacted adapter cards and platforms are listed in a warning and the operator is asked whether to proceed or not with a y/n prompt. There is no prompt if the rollback reversion is initiated via SNMP or if the **now** keyword is used. The following are examples of adapter card and fixed platform commands that may generate a warning:

- config>card>card-type
- config>card>mda
- config>card>mda>mda-type

While the 7705 SAR is processing a rollback **revert** command, CLI and SNMP commands from other users are still accepted and applied to the system. The only commands that are blocked during this process are other rollback commands including **revert**, **save**, and **compare**. Only one rollback command can be processed at a time.

Performing a rollback reversion does not have any effect on existing rollback checkpoint and rescue files; files are not renumbered or deleted. For example, if an operator reverts to rollback checkpoint file 3, the file remains as *.rb.3. If the operator then executes a rollback **save** command, the current configuration is saved as the latest rollback (extension *.rb) and *.rb.3 is incremented to *.rb.4. In this scenario, both the latest rollback checkpoint file and checkpoint file 3 will have the same configuration information.

Currently running or scheduled CRON jobs are handled like all other configurations during a rollback reversion. The CRON configuration will revert to the configuration at the time the checkpoint was created.

The **boot-good-exec** or **boot-bad-exec** commands must be manually executed after a rollback reversion; they are not automatically run.

3.9.2.1 Rollback restrictions

Some hardware or software changes can prevent operators from performing the rollback or can affect the operation of the node following the reversion.

If hardware is removed or changed after a rollback checkpoint file is saved, the node may not function as expected after the system reverts to that configuration. There is no effect if new hardware is added into previously empty slots.

A CLI rollback reversion is not supported if the rollback checkpoint file was saved in a previous major software load or if it was saved in a more recent major or minor software load. For example:

- a node running Release 20.4.R1 cannot revert to a checkpoint file saved in Release 9.0.R4
- a node running Release 9.0.R4 cannot revert to a checkpoint file saved in Release 20.4.R1

- a node running Release 9.0.R4 cannot revert to a checkpoint file saved in Release 9.0.R6

CLI rollback reversion is supported if the checkpoint file was saved in a previous minor software release. For example, a node running Release 9.0.R6 can revert to a checkpoint file saved in Release 9.0.R4. It is also supported after an operator performs an **admin reboot** or changes the primary configuration and then performs an **admin reboot**. The reboot does not remove any previously saved rollback files.

If the system runs out of memory during a CLI rollback reversion, the process aborts and the node remains in an indeterminate configuration state. The CLI screen displays a warning message that the CLI reversion failed.

A CLI rollback reversion may also fail in rare cases if the node requires a long time to complete the configuration changes. If the CLI rollback reversion fails during execution, it should be attempted again. The second attempt typically completes the remaining configuration changes.

A high availability CSM switchover during a rollback reversion will cause the rollback process to abort, and the newly active CSM will have an indeterminate configuration. This may not be immediately obvious if the CLI rollback reversion was nearly complete when it was interrupted. To assist operators, a log event is created and the results of the last rollback reversion can be displayed with the **show system rollback** command. If a high availability switchover occurs during a rollback (or within a few seconds of a rollback completing), the Last Revert Result field will display Interrupted and the operator is advised to repeat the rollback revert operation to the same checkpoint.

> **Caution:**
> - Although the use of the <Ctrl-c> key combination is not recommended during a rollback revert, it is supported in the CLI and SNMP. Interrupting a rollback **revert** command may leave the router in an indeterminate state between the active and saved configuration.
> - If <Ctrl-c> is used during a CLI rollback reversion, the 7705 SAR displays a warning message to indicate that the operator must examine the configuration and potentially issue another rollback **revert** command to return to a known, complete configuration.

3.10 Transactional configuration

Transactional configuration allows a user to make configuration changes inside a candidate configuration without actually causing changes to the active or operational configuration of the router. When the candidate configuration is complete, the user can explicitly commit the changes and cause the new configuration to become active. Transactional configuration gives the user better control and visibility over their router configurations and reduces operational risk while increasing flexibility.

Transactional configuration and CLI configuration rollback combine to provide the operational model depicted in Figure 3: Router configuration with rollback and transactions.

Figure 3: Router configuration with rollback and transactions
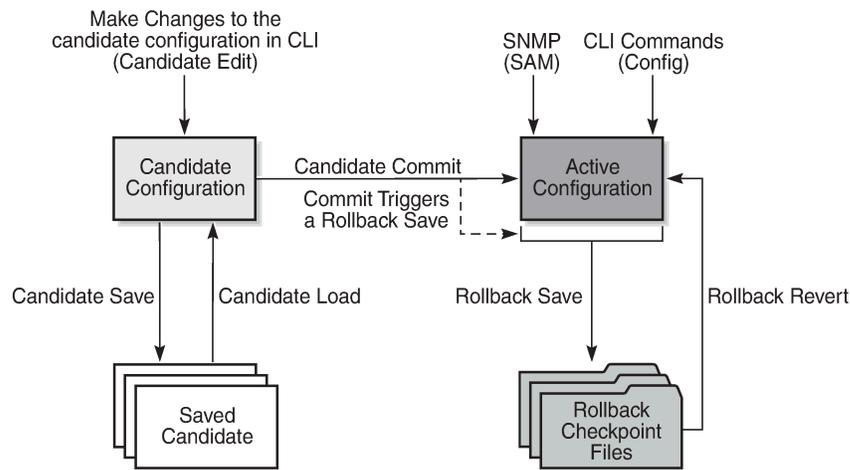
3.10.1 Basic operation

To edit the candidate configuration, the user must first enter candidate edit mode with the **candidate**>**edit** command. The user can enter and quit candidate edit mode as many times as they need before committing the candidate configuration.

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

Just as there is a single operational active configuration that can be modified simultaneously by multiple users, there is also a single global candidate configuration instance. All users make changes in the same global candidate configuration and any command that affects the candidate configuration (such as a **save** or **commit**) applies to the changes made by all users.

Users can enter an exclusive candidate edit mode by blocking other users, or sessions of the same user, from entering candidate edit mode.

When a candidate configuration is committed, the user can request an additional confirmation of the configuration. If the confirmation is not given with the **confirm** command within the specified time frame, the router automatically reverts to a configuration state before the candidate configuration changes were applied. If this automatic reversion occurs, the candidate configuration is not cleared and users can continue to edit it and try the commit later.

If the commit operation is successful and the **confirm** command is issued (if requested during the commit), all the candidate changes take operational effect and the candidate configuration is cleared. If there is an error processing the commit, the router returns to a configuration state before the candidate changes were applied. The candidate configuration is not cleared and users can continue to edit it and try the commit later.

A candidate commit may fail for various reasons, including:

*   misordering — the candidate configuration has changes that are not in the correct order; for example, an object is referred to before it is actually created

- invalid options and combinations — although many syntax errors are eliminated during the candidate editing process, the candidate configuration may contain combinations of configurations and options that are not valid and are rejected when the 7705 SAR attempts to have them take operational effect

- resource exhaustion — the application of the candidate configuration may exhaust various system resources, such as queue resources

If a commit fails, the system generates error messages to help the user correct the candidate configuration.

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

Candidate edit mode is primarily intended for building a candidate configuration using commands from the **configure** branch of the CLI. Although many CLI commands in other branches are supported, access to some CLI commands and branches are blocked, including:

- **exec** command

- **enable-admin** command

- **admin** branch

- **bof** branch

- **debug** branch

- **tools** branch

The candidate configuration can be saved to a file and loaded into a new candidate configuration later. A saved candidate file is similar to, but not exactly the same as, a 7705 SAR configuration file generated with an **admin save** command. The saved candidate file cannot be used as a configuration file and may not execute without failures.

There is no SNMP access to the candidate configuration and no SNMP management of candidates. However, when a candidate configuration is committed, any changes to the active or operational configuration are reported via the standard 7705 SAR SNMP change traps. Basic candidate status information is also available via SNMP.

The active or operational configuration can still be modified with standard CLI or SNMP commands that take immediate effect while a candidate configuration is being created or edited or a candidate commit is being processed. While in candidate edit mode, users can view the current state of the operational configuration with the **info operational** command.

3.10.2 Transactions and rollback

Transactional configuration relies on the rollback mechanism to operate. By default, the 7705 SAR automatically creates a new rollback checkpoint after a successful candidate commit operation. The rollback checkpoint includes the new configuration changes made by the commit. An optional **no-checkpoint** keyword can be used to prevent the creation of an automatic rollback checkpoint after a successful commit. If the commit fails, no rollback checkpoint is created. If the **confirmed** option is used during the candidate commit, a rollback checkpoint is created and exists whether or not the **confirm** command is issued.

Any configurations that are not supported in a rollback **revert** are also not supported in candidate edit mode. See CLI configuration rollback for more information.

3.10.3 Authorization

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

The candidate **load** and **save** commands load and save only those items that the user is authorized to access.

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

The candidate editing commands (such as adding or removing lines) only allow the user to modify items that they are authorized to access.

The candidate **commit** and **discard** commands, along with the **admin>rollback> revert** command, impact all items in the candidate configuration and are not affected by authorization.

3.11 Basic command reference

3.11.1 Command hierarchies

- CLI root-level and global commands
- Environment commands
- Rollback commands
- Candidate commands
- Show commands

3.11.1.1 CLI root-level and global commands

```
    - back
    - clear
    - echo [text-to-echo] [extra-text-to-echo] [more-text]
    - enable-admin
    - exec [-echo] [-syntax] {filename | <<[eof-marker-string]}
    - exit [all]
    - help
    - help edit
    - help globals
    - help special-characters
    - history
    - logout
    - mrinfo          [See the 7705 SAR OAM and Diagnostics Guide for command description]
    - mstat           [See the 7705 SAR OAM and Diagnostics Guide for command description]
    - mtrace          [See the 7705 SAR OAM and Diagnostics Guide for command description]
    - oam             [See the 7705 SAR OAM and Diagnostics Guide for command description]
    - password
    - ping {ip-address | dns-name} [rapid | detail] [ttl time-to-live] [tos type-of-service]
 [size bytes] [pattern pattern] [source ip-address] [interval seconds] [{next-hop ip-
address} | {interface interface-name} | bypass-routing] [count requests] [do-not-fragment]
 [router router-instance | service-name service-name] [timeout timeout] [fc fc-name]
    - pwc [previous]
    - sleep [seconds]
    - ssh host [-l username] [router router-instance | service-name service-name] [re-exchange-
min minutes] [re-exchange-mbyte megabytes]
    - telnet [ip-address | dns-name] [port] [router router-instance]
    - telnet [ip-address | dns-name] [port] [service-name service-name]
    - traceroute {ip-address | dns-name} [ttl ttl] [wait milliseconds] [no-dns] [source ip-
address] [tos type-of-service] [router router-instance | service-name service-name]
    - tree [detail] [flat]
    - write {user | broadcast} message-string
```

```
<root>
    - configure
        - <level> (any context under configure)
            - info [detail] [operational]
```

3.11.1.2 Environment commands

```
<root>
    - environment
        - alias alias-name alias-command-name
        - no alias alias-name
        - [no] create
        - kernel -password password
        - no kernel
        - [no] more
        - reduced-prompt [no of nodes in prompt]
        - no reduced-prompt
        - [no] saved-ind-prompt
        - shell -password password
        - no shell
        - [no] suggest-internal-objects
        - terminal
            - length lines
            - width width
        - time-display {local | utc}
        - [no] time-stamp
```

3.11.1.3 Rollback commands

```
admin
    - rollback
        - compare [to source2]
        - compare source1 to source2
        - delete checkpoint-rescue
        - revert checkpoint-rescue [now]
        - save [comment comment] [rescue]
        - view [checkpoint-rescue]
```

```
admin
    - compare source1 to source2
```

```
admin
    - redundancy
        - rollback-sync
```

```
config
    - system
        - rollback
            - local-max-checkpoints number
            - no local-max-checkpoints
            - remote-max-checkpoints number
            - [no] remote-max-checkpoints
            - [no] rescue-location file-url | rescue filename
            - [no] rollback-location file-url | rollback filename
```

```
config
    - redundancy
        - [no] rollback-sync
```

© 2024 Nokia.

3.11.1.4 Candidate commands

```
candidate
    - edit [exclusive]
    - commit [confirmed timeout] [comment comment]
    - commit no-checkpoint [confirmed timeout]
    - confirm
    - copy [line]
    - delete [line]
    - discard [now]
    - goto line
    - insert [line]
    - load file-url [overwrite | insert | append]
    - quit
    - redo [count]
    - replace [line]
    - save file-url
    - undo [count]
    - view [line]
```

```
- config
    - system
        - management cli
            - configuration
                    - [no] immediate
```

3.11.1.5 Show commands

```
show
    - alias
    - system
        - candidate
```

3.11.2 Command descriptions

- CLI root-level and global commands
- Environment commands
- Candidate commands
- Rollback commands
- Show commands

3.11.2.1 CLI root-level and global commands

back

Syntax

back

Context

<global>

Description

This command moves the context back one level of the command hierarchy. For example, if the current level is the **config router mpls** context, the **back** command moves the cursor to the **config router** context level.

clear

Syntax

clear

Context

<global>

Description

This command clears statistics for a specified entity or clears and resets the entity.

Parameters

card

reinitializes an I/O module in a specified slot

cpm-filter

clears CPM filter

cron

      clears CRON history

eth-cfm

      clears ETH-CFM parameters

external-alarms

      accesses external alarms-related clear commands

filter

      clears IP filter counters

group-encryption

      accesses group encryption-related clear commands

ipsec

      accesses IPSec-related clear commands

lag

      accesses LAG-related clear commands

log

      closes and reinitializes the log specified by log-id

mda

      reinitializes the specified MDA in a particular slot

mw

      reboots managed microwave devices

port

      clears port statistics

radius

      clears the RADIUS server state

router

      accesses clear router commands affecting the router instance in which they are entered

            Values   arp, bfd, bgp, dhcp, dhcp6, forwarding-table, grt-lookup, icmp6, igmp, interface, isis, ldp, mld, mpls, neighbor, ospf, ospf3, pim, rip, router-advertisement, rsvp, vrrp

saa

      clears the SAA test results

scada

      clears SCADA statistics

screen

      clears the console or Telnet screen

security

      accesses network security-related clear commands

service

      clears service ID and statistical entities

system

       clears (re-enables) a previously failed reference

tacplus

       clears the TACACS+ server state

test-oam

       accesses OAM-related clear statistics commands

testhead

       accesses test head-related clear commands

trace

       clears the trace log

vrrp

       clears and resets the VRRP interface and statistical entities

echo

Syntax

echo [*text-to-echo*] [*extra-text-to-echo*] [*more-text*]

Context

<global>

Description

This command echoes arguments on the command line. The primary use of this command is to allow messages to be displayed to the screen in files executed with the **exec** command.

Parameters

text-to-echo

       specifies a text string to be echoed, up to 256 characters

extra-text-to-echo

       specifies more text to be echoed, up to 256 characters

more-text

       specifies more text to be echoed, up to 256 characters

enable-admin

Syntax

enable-admin

Context

Description

This command enables the user to become a system administrator.

The **enable-admin** command is in the default profile. By default, all users are granted access to this command.

> **Note:** If the **admin-password** is configured in the **config>system>security>password** context, any user can enter a special administrative mode by entering the **enable-admin** command. See the 7705 SAR System Management Guide, "Password Commands", for information about the **admin-password** command.

After the **enable-admin** command is entered, the user is prompted for a password. If the password matches, the user is granted unrestricted access to all the commands.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password are determined by the **complexity** command.

The following displays an example of the password command usage.

Example:

```
config>system>security#password
security>password# admin-password test1234 hash
security>password# aging 365
security>password# minimum-length 8
security>password# attempts 5 time 5 lockout 20
security>password# authentication-order radius tacplus local
security>password# enable-admin
Password: test1234
security>password#
```

The following example displays the password configuration:

```
ALU-1>config>system>security# info
----------------------------------------------
...
aging 365
minimum-length 8
attempts 5 time 5 lockout 20
admin-password "rUYUz9XMo6I" hash
...
----------------------------------------------
ALU-1>config>system>security#
```

There are two ways to verify that a user is in **enable-admin** mode:

- enter the **show users** command——administrator can see which users are in **enable-admin** mode, indicated by the "A" on the same line as the username

- enter the **enable-admin** command again at the root prompt and an error message returns

The # sign indicates the current session.

```
A:7705:Dut-C# show users
===========================================================================
Username                                      Type
    From
    Router instance
    Connection ID                             Login time
        Session ID          SSH Channel ID        Idle time
===========================================================================
```

```
                                              Console
    --
    --
    6                                                --
      6                           --               0d 00:03:20  --
-------------------------------------------------------------------------------
admin                                          Telnet
    192.168.192.37
    management
    8                                         03OCT2023 14:06:52
      8                           --               0d 00:01:04  --
-------------------------------------------------------------------------------
bla                                            Telnet
    192.168.192.37
    management
    9                                         03OCT2023 14:08:42
      9                           --               0d 00:00:09  A-
-------------------------------------------------------------------------------
admin                                          SSHv2
    192.168.192.37
    management
    7                                         03OCT2023 14:06:24
      #7                          0                0d 00:00:00  --
-------------------------------------------------------------------------------
Number of users: 3
Number of sessions: 3
'#' indicates the current active session
'A' indicates user is in admin mode
===============================================================================
*A:7705:Dut-C#
```

exec

Syntax

exec [**-echo**] [**-syntax**] {*filename*| **<<**[*eof-marker-string*]]}

Context

<global>

Description

This command executes the contents of a text file as if they were CLI commands entered at the console.

Exec commands do not have **no** versions.

Related commands are:

- boot-good-exec

  Use this command to configure a URL for a CLI script to exec following a successful configuration boot.

- boot-bad-exec

  Use this command to configure a URL for a CLI script to exec following a failed configuration boot.

Parameters

-echo

echoes the contents of the **exec** file to the session screen as it executes

Default echo disabled

-syntax

performs a syntax check of the file without executing the commands. Syntax checking looks for invalid commands and keywords as well as unprintable characters in configured parameters. An error message is displayed if any are found.

Default execute file commands

filename

the text file with CLI commands to execute

<<

Stdin can be used as the source of commands for the exec command. When stdin is used as the exec command input, the command list is terminated with <Ctrl-c>, "EOF<Return>" or "*eof_string*<Return>".

If an error occurs entering an exec file sourced from stdin, all commands after the command returning the error are silently ignored. The exec command indicates the command error line number when the stdin input is terminated with an end-of-file input.

eof-marker-string

The ASCII printable string used to indicate the end of the exec file when stdin is used as the exec file source. <Ctrl-c> and "EOF" can always be used to terminate an exec file sourced from stdin.

Default <Ctrl-c>, EOF

exit

Syntax

exit [**all**]

Context

<global>

Description

This command returns to the context from which the current level was entered. For example, if you navigated to the current level on a context by context basis, then the **exit** command only moves the cursor back one level.

```
ALU-1# configure
ALU-1>config# router
ALU-1>config>router# mpls
ALU-1>config>router>mpls# exit
ALU-1>config>router# exit
ALU-1>config# exit
```

If you navigated to the current level by entering a command string, then the **exit** command returns the cursor to the context in which the command was initially entered.

```
ALU-1# configure router mpls
ALU-1>config>router>mpls# exit
ALU-1#
```

The **exit all** command moves the cursor all the way back to the root level.

```
ALU-1# configure
ALU-1>config# router
ALU-1>config>router# mpls
ALU-1>config>router>mpls# exit all
ALU-1#
```

Parameters

all

exits back to the root CLI context

help

Syntax

help

help edit

help globals

help special-characters

Context

<global>

Description

This command provides a brief description of the help system. The following information is displayed:

```
Help may be requested at any point by hitting a question mark '?'.
In case of an executable node, the syntax for that node will be displayed with an
explanation of all parameters.
In case of sub-commands, a brief description is provided.
Global Commands:
     Help on global commands can be observed by issuing "help globals" at any time.
Editing Commands:
     Help on editing commands can be observed by issuing "help edit" at any time.
```

Parameters

help

displays a brief description of the help system

help edit

displays help on editing

Available editing keystrokes:

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

help globals

displays help on global commands

Available global commands:

```
back            - Go back a level in the command tree
candidate       + Commands used for editing candidate configurations
echo            - Echo the text that is typed in
enable-admin    - Enable the user to become a system administrator
exec            - Execute a file - use -echo to show the commands and
                  prompts on the screen
exit            - Exit to intermediate mode - use option all to exit to
                  root prompt
help            - Display help
history         - Show command history
logout          - Log off this system
mrinfo          - Request multicast router information
mstat           - Trace multicast path from a source to a receiver and
                  display multicast packet rate and loss information
mtrace          - Trace multicast path from a source to a receiver
oam             + OAM Test Suite
ping            - Verify the reachability of a remote host
pwc             - Show the present working context
sleep           - Sleep for specified number of seconds
ssh             - SSH to a host
telnet          - Telnet to a host
traceroute      - Determine the route to a destination address
tree            - Display command tree structure from the context of
                  execution
write           - Write text to another user
```

help special-characters

displays help on special characters

Use the following CLI commands to display more information about commands and command syntax:

?

lists all commands in the current context

string?

lists all commands available in the current context that start with the string

command ?

displays command syntax and associated keywords

string\<Tab\> or string\<Space\>

completes a partial command name (auto-completion) or lists available commands that match the string

history

Syntax

history

Context

\<global\>

Description

This command lists the last 30 commands entered in this session.

Re-execute a command in the history with the **!n** command, where **n** is the line number associated with the command in the history output.

For example:

```
ALU-1# history
      68 info
      69 exit
      70 info
      71 filter
      72 exit all
      73 configure
      74 router
      75 info
      76 interface "test"
      77 exit
      79 info
      80 interface "test"
      81 exit all
      82 configure router
      83 interface
      84 info
      85 interface "test"
      86 info
      87 exit all
      88 configure
      89 card 1
      91 exit
      92 router
      93 exit
      94 history
ALU-1# !88
ALU-1# configure
ALU-1>config#
```

info

Syntax

info [**detail**] [**operational**]

Context

configure

Description

This command displays the running configuration for the configuration context. It can be used at any level under **configure** but not at the top **configure** level.

The output of this command is similar to the output of a **show config** command. This command, however, lists the configuration of the context where it is entered and all branches below that context level.

For example:

```
ALU-1>config>router>mpls# info
----------------------------------------
mpls
            interface "system"
            exit
            interface "to_1/2/1"
                label-map 131
                    pop
                    no shutdown
                exit
            exit
            static-lsp "to121"
                to 10.8.8.8
                push 121 nexthop 10.1.3.1
                no shutdown
            exit
            no shutdown
        exit
    exit
----------------------------------------------
ALU-1>config>router>mpls#
```

By default, the command only enters the configuration parameters that vary from the default values. The **detail** keyword causes all configuration parameters to be displayed.

The **operational** keyword is used to display the operational configuration of the current configuration context when the user is in candidate edit mode. The **operational** keyword is mandatory when using the **info** command while in candidate edit mode.

Parameters

detail

displays all configuration parameters, including parameters at their default values

operational

displays the operational configuration of the current configuration context

logout

Syntax

logout

Context

<global>

Description

This command logs out of the router session.

When the **logout** command is issued from the console, the login prompt is displayed and any log IDs directed to the console are discarded. When the console session resumes (regardless of the user), the log output to the console resumes.

When a Telnet session is terminated from a **logout** command, all log IDs directed to the session are removed. When a user logs back in, the log IDs must be recreated.

password

Syntax

password

Context

<ROOT>

Description

This command changes a user CLI login password.

When a user logs in after the administrator forces a **new-password-at-login,** or the password has expired (**aging**), then this command is automatically invoked.

When invoked, the user is prompted to enter the old password, the new password, and then the new password again to verify the correct input.

If a user fails to create a new password after the administrator forces a **new-password-at-login** or after the password has expired, the user is not allowed access to the CLI.

ping

Syntax

ping {*ip-address* | *dns-name*} [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *seconds*] [{**next-hop** *ip-address*} | {**interface** *interface-name*} | **bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance* | **service-name** *service-name*] [**timeout** *timeout*] [**fc** *fc-name*]

Context

<global>

Description

This command is the TCP/IP utility to verify IP reachability.

Parameters

ip-address

the IP address of the remote host to ping

source *ip-address*

the source IP address to use in the ping requests

> **Default**   the IP address of the egress IP interface

next-hop *ip-address*

this option disregards the routing table and sends this packet to the specified next hop address. This address must be on an adjacent router that is attached to a subnet that is common between this and the next-hop router.

> **Values**   a valid IP next hop IP address

> **Default**   per the routing table

dns-name

the DNS name (if DNS name resolution is configured) of the remote host to ping

> **Values**   128 characters maximum

rapid | detail

the **rapid** parameter specifies to send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the **count** option.

The **detail** parameter includes in the output the interface on which the ping reply was received.

```
ALU-1# ping 192.168.xx.xx4 detail
PING 192.168.xx.xx4: 56 data bytes
64 bytes from 192.168.xx.xx4 via fei0: icmp_seq=0 ttl=64 time=0.000 ms.
64 bytes from 192.168.xx.xx4 via fei0: icmp_seq=1 ttl=64 time=0.000 ms.
64 bytes from 192.168.xx.xx4 via fei0: icmp_seq=2 ttl=64 time=0.000 ms.
64 bytes from 192.168.xx.xx4 via fei0: icmp_seq=3 ttl=64 time=0.000 ms.
64 bytes from 192.168.xx.xx4 via fei0: icmp_seq=4 ttl=64 time=0.000 ms.
---- 192.168.xx.xx4 PING Statistics ----
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max/stddev = 0.000/0.000/0.000/0.000 ms
ALU-1#
```

time-to-live

the IP Time To Live (TTL) value to include in the ping request, expressed as a decimal integer

Values   0 to 128

type-of-service

the type-of-service (ToS) bits in the IP header of the ping packets, expressed as a decimal integer

Values   0 to 255

bytes

the size in bytes of the ping request packets

Values   0 to 65507

Default   56 bytes (actually 64 bytes because 8 bytes of ICMP header data is added to the packet)

pattern

16-bit pattern string to include in the ping packet, expressed as a decimal integer

Values   0 to 65535

seconds

the interval in seconds between consecutive ping requests, expressed as a decimal integer

Values   1 to 10000

Default   1

interface-name

specifies the interface name

bypass-routing

sends the ping request to a host on a directly attached network bypassing the routing table. The host must be on a directly attached network or an error is returned.

requests

the number of ping requests to send to the remote host, expressed as a decimal integer

Values   1 to 10000

Default   5

do-not-fragment

specifies that the request frame should not be fragmented. This option is particularly useful in combination with the size parameter for maximum MTU determination.

router-instance

specifies the router name or service ID

Values   *router-name*: Base, management

service-id: 1 to 2147483647

Basic System Configuration Guide Release 24.4.R1   CLI usage

Default   Base

service-name

specifies the service name, 64 characters maximum

timeout

specifies the timeout in seconds

Values   1 to 10

Default   5

fc-name

specifies the forwarding class

Values   be | l2 | af | l1 | h2 | ef | h1 | nc

Default   nc

pwc

Syntax

pwc [**previous**]

Context

<global>

Description

This command displays the present or previous working context of the CLI session.

The **pwc** command provides a user who is in the process of dynamically configuring a chassis a way to display the current or previous working context of the CLI session. The **pwc** command displays a list of the CLI nodes that hierarchically define the current context of the CLI instance of the user.

For example:

```
A:ALU>config>router>mpls# pwc
----------------------------------------------
Present Working Context :
----------------------------------------------
 <root>
  configure
  router "Base"
  mpls
----------------------------------------------
A:ALU>config>router>mpls#
```

When the **previous** keyword is specified, the previous context is displayed. This is the context entered by the CLI parser upon execution of the **exit** command. The current context of the CLI is not affected by the **pwc** command.

3HE 20393 AAAA TQZZA   62

© 2024 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Parameters

previous

displays the previous working context

sleep

Syntax

sleep [*seconds*]

Context

<global>

Description

This command causes the console session to pause operation (sleep) for 1 second (default) or for the specified number of seconds.

Parameters

seconds

specifies the number of seconds for the console session to sleep, expressed as a decimal integer

Values   1 to 100

Default   1

ssh

Syntax

ssh *host* [**-l** *username*] [**router** *router-instance* | **service-name** *service-name*] [**re-exchange-min** *minutes*] [**re-exchange-mbyte** *megabytes*]

Context

<global>

Description

This command opens a Secure Shell (SSH) session with another host.

The command initiates a client SSH session with the remote host and is independent from the administrative or operational state of the SSH server. However, to be the target of an SSH or SFTP session, the SSH server must be operational.

The command also allows the user to initiate an SSH session with a key re-exchange to occur after a specified number of minutes have passed or a specified number of megabytes have been transmitted. If both parameters are configured, the key re-exchange occurs at whatever limit is reached first. If neither parameter is set, key re-exchange does not occur.

Quitting SSH while in the process of authentication is accomplished by either executing a <Ctrl-c> or tilde and dot "(~.")", assuming the "~" is the default escape character for the SSH session.

Parameters

host

the remote host for an SSH session. The IP address, DNS name (if DNS name resolution is configured), or the username at the IP address can be specified.

For IPv6 addresses, including the "*-interface*" for the link local address is mandatory; otherwise, "*-interface*" is omitted. For example, if the *user* is "alu_admin" and the IPv6 *hostname* consists of 2001:db8:a0b:12f0::1 along with the link local interface "ies1_chicago", the full command would be (note the "-" between the *ipv6-address* and the *interface*):

ssh -l *alu_admin 2001:db8:a0b:12f0::1-ies1_chicago*

Values	[*user@*]*hostname:*	255 characters maximum
	user:	username, 32 characters maximum
	hostname:	[*dns-name* | *ipv4-address* | *ipv6-address*]
	dns-name:	128 characters maximum
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x[*-interface*]
		x:x:x:x:x:x:d.d.d.d[*-interface*]
		x: [0 to FFFF]H
		d: [0 to 255]D
		interface — 32 chars max, mandatory for link local addresses

username

the username to use when opening the SSH session

router-instance

the router name or service ID

Values	*router-name:* Base, management
	service-id: 1 to 2147483647

Default	Base

service-name

the service name, 64 characters maximum

minutes

specifies the time interval after which the SSH client initiates the key re-exchange

Values   1 to 1440

Default   60

megabytes

specifies the number of megabytes transmitted during an SSH session after which the SSH client initiates the key re-exchange

Values   1 to 64000

Default   1024

telnet

Syntax

telnet [*ip-address* | *dns-name*] [*port*] [**router** *router-instance*]

telnet [*ip-address* | *dns-name*] [*port*] [**service-name** *service-name*]

Context

<global>

Description

This command opens a Telnet session to a remote host.

Telnet servers in 7705 SAR networks limit a Telnet client to three retries to log in. The Telnet server disconnects the Telnet client session after three retries. The number of retry attempts for a Telnet client session is not user-configurable.

Parameters

ip-address

the IP address of the remote host

dns-name

the DNS name (if DNS name resolution is configured) of the remote host

Values   128 characters maximum

port

the TCP port number to use to Telnet to the remote host, expressed as a decimal integer

Values   1 to 65535

Default   23

router-instance

the router name or service ID

Values   *router-name*: Base, management

service-id: 1 to 2147483647

> **Default**   Base

service-name

> specifies the service name, 64 characters maximum

traceroute

Syntax

traceroute {*ip-address*| *dns-name*} [**ttl** *ttl*] [**wait** *milliseconds*] [**no-dns**] [**source** *ip-address*] [**tos** *type-of-service*] [**router** *router-instance* | **service-name** *service-name*]

Context

<global>

Description

The TCP/IP traceroute utility determines the route to a destination address. Aborting a traceroute with the <Ctrl-c> command could require issuing a second <Ctrl-c> command before the prompt is returned.

```
ALU-1# traceroute 192.168.xx.xx4
traceroute to 192.168.xx.xx4, 30 hops max, 40 byte packets
 1  192.168.xx.xx4 0.000 ms  0.000 ms  0.000 ms
ALU-1#
```

Parameters

ip-address

> the IP address to trace

dns-name

> the DNS name (if DNS name resolution is configured)

> > **Values**   128 characters maximum

ttl

> the maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer

> > **Values**   1 to 255

milliseconds

> the time in milliseconds to wait for a response to a probe, expressed as a decimal integer

> > **Values**   1 to 60000

> > **Default**   5000

no-dns

when the **no-dns** keyword is specified, a DNS lookup for the specified hostname does not perform

> **Default**   DNS lookups are performed

source *ip-address*

the source IP address to use as the source of the probe packets. If the IP address is not one of the device's interfaces, an error is returned.

type-of-service

the type-of-service (ToS) bits in the IP header of the probe packets, expressed as a decimal integer

> **Values**   0 to 255

router-instance

the router name or service ID

> **Values**   *router-name*: Base, management
>
> *service-id:* 1 to 2147483647

> **Default**   Base

service-name

specifies the service name, 64 characters maximum

tree

Syntax

tree [**detail**] [**flat**]

Context

<global>

Description

This command displays the command hierarchy structure from the present working context.

Parameters

detail

includes parameter information for each command displayed in the tree output

flat

displays the command hierarchy on single lines

write

Syntax

write {*user* | **broadcast**} *message-string*

Context

<global>

Description

This command sends a console message to a specific user or to all users with active console sessions.

Parameters

user

the name of a user with an active console session to which to send a console message

Values   any valid CLI username

broadcast

specifies that the *message-string* is to be sent to all users logged in to the router

message-string

the message string to send, up to 250 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

3.11.2.2 Environment commands

alias

Syntax

alias *alias-name alias-command-name* **no alias** *alias-name*

Context

environment

Description

This command enables the substitution of a command line by an alias.

Use the **alias** command to create alternative names for an entity or command string that are easier to understand and remember. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes. The special characters "/" and "\" cannot be used as the first character inside an alias string. Only a single command can be present in the command string.

The **alias** command can be entered in any context but must be created in the **root>environment** context.

For example, to create an alias named **soi** to display MPLS interfaces, enter:

alias soi "show router mpls interface"

An alias can contain embedded quotes if the quote is preceded with the "\" character (for example, **alias my-alias "| match \"***string***\""**). This enables aliases to be created as shortcuts for complex commands; for example:

environment alias my-summary "| match expression \"----|Description|Interface|Admin State| Oper State|Transceiver Type|Optical Compliance|Link Length\" | match invert-match expression \"Ethernet Interface|OTU Interface\" | match invert-match expression \"----\" post-lines 1"

When applied to the **show port 1/1/1 detail** command, **show port 1/1/1 detail my-summary** displays only the output fields that match the conditions in the match expression as shown in the following examples:

Without alias:

```
*A:Sar18 Dut-B# show port 1/1/1 detail
===============================================================================
Ethernet Interface
===============================================================================
Description       : 10/100/Gig Ethernet SFP
Interface         : 1/1/1                  Oper Speed       : 1 Gbps
Link-level        : Ethernet               Config Speed     : 1 Gbps
Admin State       : up                     Oper Duplex      : full
Oper State        : up                     Config Duplex    : full
Physical Link     : Yes                    MTU              : 1572
Single Fiber Mode : No
IfIndex           : 35684352               Hold time up     : 0 seconds
Last State Change : 05/23/2018 18:41:28    Hold time down   : 0 seconds
Last Cleared Time : N/A                    DDM Events       : Enabled
Phys State Chng Cnt: 1
Configured Mode   : network                Encap Type       : 802.1q
Dot1Q Ethertype   : 0x8100                 QinQ Ethertype   : 0x8100
Ing. Pool % Rate  : 100                    Egr. Pool % Rate : 100
Net. Egr. Queue Pol: default
Net. Scheduler Mode: 16-priority
Auto-negotiate    : true                   MDI/MDX          : unknown
Config Phy-tx-clock: auto-pref-slave       Oper Phy-tx-clock: N/A
NetEgr.Unshaped-Cir: 0 Kbps
Allow Eth-BN      : False
Egress Rate       : Default                Ingress Rate     : Default
Egr.Rate Incl.FCS : Disabled
Ingress CBS(bytes) : 130816                Src-pause        : Disabled
                                           LACP Tunnel      : Disabled
Down-when-looped  : Disabled               Keep-alive       : 10
Loop Detected     : False                  Retry            : 120
Use Broadcast Addr : False
Loopback          : none                   Swap Mac Addr    : Disabled
Loopback Time Left : unspecified
Cfm Loopback      : Disabled
PTP Asymmetry     : 0                      Edge Timestamp   : Disable
Timestamp Capable : True
Sync. Status Msg. : Disabled               Rx Quality Level : N/A
Tx DUS/DNU        : Disabled               Tx Quality Level : N/A
SSM Code Type     : sdh
CRC Mon SD Thresh : Disabled               CRC Mon Window   : 10 seconds
CRC Mon SF Thresh : Disabled
EFM OAM           : Disabled               EFM OAM Link Mon : Disabled
Configured Address : d6:65:01:01:00:01
Hardware Address  : d6:65:01:01:00:01
Group Encryption
Inbound Keygroup Id : N/A
Inbound Keygroup Id : N/A
Transceiver Data
```

```
Transceiver Status : operational
Transceiver Type   : Unknown
Model Number       : none
TX Laser Wavelength: 0 nm                     Diag Capable       : no
Connector Code     : Unknown                  Vendor OUI         : 00:00:00
Manufacture date   : 2000/01/01               Media              : Ethernet
Serial Number      : none
Part Number        : none
Optical Compliance :
Link Length support: Unknown
SFP Sync-E Capable : yes
...
```

With alias:

```
*A:Sar18 Dut-B# show port 1/1/1 detail my-summary
Description        : 10/100/Gig Ethernet SFP
Interface          : 1/1/1                    Oper Speed         : 1 Gbps
Admin State        : up                       Oper Duplex        : full
Oper State         : up                       Config Duplex      : full
Transceiver Type   : Unknown
Optical Compliance :
Link Length support: Unknown
-------------------------------------------------------------------------
*A:Sar18 Dut-B#
```

Parameters

alias-name

> the alias name. Do not use a valid command string for the alias. If the alias specified is an actual command, this causes the command to be replaced by the alias.

alias-command-name

> the command line to be associated

create

Syntax

[**no**] **create**

Context

environment

Description

By default, the **create** command is required to create a new OS entity.

The **no** form of the command disables requiring the **create** keyword.

Default

create

kernel

Syntax

kernel -password *password*

no kernel

Context

environment

Description

This command enables and disables the kernel.

Parameters

password

specifies the password to access the kernel, up to 256 characters

more

Syntax

[**no**] **more**

Context

environment

Description

This command enables per-screen CLI output, meaning that the output is displayed on a screen-by-screen basis. The terminal screen length can be modified with the terminal command.

The following prompt appears at the end of each screen of paginated output:

```
Press any key to continue (Q to quit)
```

The **no** form of the command displays the output all at once. If the output length is longer than one screen, the entire output is displayed, which may scroll the screen.

Default

more

reduced-prompt

Syntax

reduced-prompt [*no of nodes in prompt*]

no reduced-prompt

Context

environment

Description

This command configures the maximum number of higher CLI context levels to display in the CLI prompt for the current CLI session. This command is useful when configuring features that are several node levels deep, which can cause the CLI prompt to become too long.

By default, the CLI prompt displays the system name and the complete context in the CLI.

The number of nodes specified indicates the number of higher-level contexts that can be displayed in the prompt.

For example, if **reduced-prompt** is set to 2, the two highest contexts from the present working context are displayed by name with the hidden (reduced) contexts compressed into a ellipsis ("…").

```
ALU-1>environment# reduced-prompt 2
ALU-1>config>router# interface to-103
ALU-1>...router>if#
```

The setting is not saved in the configuration. It must be reset for each CLI session or stored in an **exec** script file.

The **no** form of the command reverts to the default.

Default

no reduced-prompt

Parameters

no-of-nodes-in-prompt

the maximum number of higher-level nodes displayed by name in the prompt, expressed as a decimal integer

Values   0 to 15

Default   2

saved-ind-prompt

Syntax

[**no**] **saved-ind-prompt**

Context

environment

Description

This command enables a saved indicator in the prompt. When changes are made to the configuration file, a "*" appears in the prompt string indicating that the changes have not been saved. When an admin **save** command is executed, the "*" disappears.

```
*A:ALU-48# admin save
Writing file to ftp://192.0.2.43/./sim48/sim48-config.cfg
Saving configuration .... Completed.
A:ALU-48
```

Default

saved-ind-prompt

shell

Syntax

shell -password *password*

no shell

Context

environment

Description

This command enables and disables the shell.

Parameters

password

specifies the password to enter the shell, up to 256 characters

suggest-internal-objects

Syntax

[**no**] **suggest-internal-objects**

Context

environment

Description

This command enables the suggestion of internally created objects while auto-completing in the CLI.

Default

no suggest-internal-objects

terminal

Syntax

terminal

Context

environment

Description

This command enables the context to configure the terminal screen length and width for the current CLI session. The terminal length and width cannot be configured for Telnet or SSH sessions, as the correct display size is automatically negotiated.

length

Syntax

length *lines*

Context

environment>terminal

Description

This command sets the terminal screen length (number of lines).

Default

24 — terminal dimensions are set to 24 lines long by 80 characters wide

Parameters

lines

the number of lines for the terminal screen length

Values   1 to 512

width

Syntax

width *width*

Context

environment>terminal

Description

This command sets the terminal screen width (number of characters).

Default

80 — terminal dimensions are set to 24 lines long by 80 characters wide

Parameters

width

the number of characters for the terminal screen width

Values   1 to 512

time-display

Syntax

time-display {**local** | **utc**}

Context

environment

Description

This command displays timestamps in the CLI session based on local time or Coordinated Universal Time (UTC).

The system keeps time internally in UTC and is capable of displaying the time in either UTC or local time based on the time zone configured.

This configuration command is only valid for times displayed in the current CLI session. This includes displays of event logs, traps and all other places where a timestamp is displayed.

In general, all timestamps are shown in the time selected. This includes log entries destined for console/ session, memory, or SNMP logs. Log files on compact flash are maintained and displayed in UTC format.

Default

time-display local

time-stamp

Syntax

[**no**] **time-stamp**

Context

environment

Description

This command displays timestamps before the CLI prompt, indicating the last time that the command was completed. The date and time are displayed; the time format is either local or UTC, depending on how it was set with the **time-display** command.

Default

no time-stamp

3.11.2.3 Candidate commands

candidate

Syntax

candidate

Context

<root>

Description

This command enables the context to edit candidate configurations and must preface every command in the **candidate** CLI branch.

Commands in the **candidate** CLI branch, except for the **edit** command, are available only when in candidate edit mode.

Default

n/a

edit

Syntax

edit [**exclusive**]

Context

candidate

Description

This command enables the candidate edit mode where changes can be made to the candidate configuration and sets the edit point to the end of the candidate. The edit point is the point after which new commands are inserted into the candidate configuration. In candidate edit mode, the CLI prompt displays edit-cfg near the root of the prompt. All other commands in the **candidate** CLI branch are blocked until the user enters candidate edit mode.

The **exclusive** parameter allows the user to modify the candidate configuration and block all other users (and other sessions of the same user) from entering candidate edit mode. This parameter can only be used if the candidate configuration is empty and no user is already in candidate edit mode. Before quitting exclusive candidate edit mode, the user must either commit or discard their changes. If the user commits a candidate configuration with the **confirmed** option while in exclusive candidate edit mode, the exclusive lock is removed during the countdown time to allow any user to confirm the changes.

If the CLI session times out while the user is in exclusive candidate edit mode, the contents of the candidate configuration are discarded. If the user has the candidate configuration locked, the **admin disconnect** command can be used to forcibly disconnect them and to clear the contents of the candidate.

Default

n/a

Parameters

exclusive

enables exclusive candidate edit mode

commit

Syntax

commit [**confirmed** *timeout*] [**comment** *comment*]

commit no-checkpoint [**confirmed** *timeout*]

Context

candidate

Description

This command applies the changes in the candidate configuration to the active or operational configuration.

When a candidate configuration is committed, the **confirmed** keyword can be used to require an additional confirmation, which is useful when changes are being made that could impact management reachability to the router. The contents of the candidate configuration remain visible but cannot be edited until the timeout is completed or the commit is confirmed. If the confirmation is not given with the **confirm** command within the configured timeout period, the router automatically reverts to a configuration state before the candidate configuration changes were applied.

Standard line-by-line, non-transactional configuration commands (including via SNMP) are not blocked during the countdown period, but any changes made to the configuration during the countdown period are rolled back if the timeout expires.

A rollback **revert** is blocked during the countdown period until the commit has been confirmed.

If the commit operation is successful, all the candidate changes take operational effect and the candidate configuration is cleared. If there is an error processing the commit, or if the candidate **confirm** command is not issued and an auto-revert occurs, the router automatically reverts to a configuration state before the candidate configuration changes were applied. If the automatic reversion occurs, the candidate configuration is not cleared and users can continue to edit it and try the commit later.

By default, the 7705 SAR automatically creates a new rollback checkpoint after a successful commit operation that contains the new configuration changes made by the commit. The rollback checkpoint remains available even if the commit is not confirmed. The **no-checkpoint** keyword allows users to commit the candidate configuration without creating a rollback checkpoint.

A commit operation is blocked if a rollback **revert** is currently being processed.

Default

n/a

Parameters

confirmed

> requires the **confirm** command to be issued before the end of the timeout period to avoid an auto-revert of the configuration

timeout

> the auto-revert timeout period, in minutes

> > **Values**   1 to 168

no-checkpoint

> blocks the creation of a rollback checkpoint for a successful commit

comment

> a string up to 255 characters in length describing the automatic rollback checkpoint file

confirm

Syntax

confirm

Context

candidate

Description

This command is used to confirm a candidate configuration. If the optional **confirmed** parameter is used with the **commit** command, this command must be issued before the timeout period expires; otherwise, the router automatically reverts to a configuration state before the candidate configuration changes were applied. After the automatic reversion, the candidate configuration remains available for editing and a subsequent commit.

During the countdown, the contents of the candidate remain visible with the candidate **view** command but changes to the candidate are blocked until the timeout is completed or this command is issued.

This command also clears the contents of the candidate configuration and allows users to enter candidate edit mode again.

Default

n/a

copy

Syntax

copy [*line*]

Context

candidate

Description

This command copies the selected CLI branch, including all sub-branches, into a temporary buffer that can be used with a subsequent **insert** command. The contents of the temporary buffer are deleted when the operator exits candidate edit mode. Line numbers can be displayed with the **candidate view** command.

Default

edit-point

Parameters

line

specifies which line to copy

Values   *line* | *offset* | **first** | **edit-point** | **last**

line — the absolute line number

offset — the line relative to the current edit point, prefixed with either + or - to indicate before or after the current edit point

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not "exit"

delete

Syntax

delete [*line*]

Context

candidate

Description

This command deletes the selected CLI branch, including all sub-branches. The deleted lines are also copied into a temporary buffer that can be used with a subsequent **insert** command. Line numbers can be displayed with the **candidate view** command.

Default

edit-point

Parameters

line

specifies which line to delete

Values *line* | *offset* | **first** | **edit-point** | **last**

line — the absolute line number

offset — the line relative to the current edit point, prefixed with either + or - to indicate before or after the current edit point

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not "exit"

discard

Syntax

discard [**now**]

Context

candidate

Description

This command deletes the entire contents of the candidate configuration and exits candidate edit mode. The **undo** command cannot be used to recover a candidate configuration that has been discarded with this command.

Default

n/a

Parameters

now

deletes the candidate configuration with no confirmation prompt for the discard

goto

Syntax

goto *line*

Context

candidate

Description

This command changes the edit point of the candidate configuration. The edit point is the point after which new commands are inserted into the candidate configuration as an operator navigates the CLI and issues commands in candidate edit mode. Line numbers can be displayed with the **candidate view** command.

Default

edit-point

Parameters

line

specifies which line is to be the edit point for the insertion of new commands

Values   *line* | *offset* | **first** | **edit-point** | **last**

line — the absolute line number

offset — the line relative to the current edit point, prefixed with either + or - to indicate before or after the current edit point

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not "exit"

insert

Syntax

insert [*line*]

Context

candidate

Description

This command inserts the contents of the temporary buffer (populated with a previous **copy** or **delete** command) into the candidate configuration. The operator can specify any line in the candidate configuration to be the insertion point, but by default, the contents are inserted after the current edit point. The contents of the temporary buffer are deleted when the operator exits candidate edit mode.

Insertions are context-aware. The temporary buffer always stores the CLI context (such as the current CLI branch) for each line deleted or copied. If the contents to be inserted are supported at the context of the insertion point, they are simply inserted into the configuration. If the contents to be inserted are not supported at the context of the insertion point, the following actions are automatically performed by the system:

1. The context at the insertion point is closed using multiple exit statements.

2. The context of the lines to be inserted is built (added) into the candidate configuration at the insertion point.

3. The contents of the temporary buffer are added.

4. The context of the inserted lines is closed using exit statements.

5. The context from the original insertion point is rebuilt, leaving the context at the same point as it was before the insertion.

Line numbers can be displayed with the **candidate view** command.

Default

edit-point

Parameters

line

specifies where to insert the contents of the temporary buffer

Values *line* | *offset* | **first** | **edit-point** | **last**

line — the absolute line number

offset — the line relative to the current edit point, prefixed with either + or - to indicate before or after the current edit point

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not "exit"

load

Syntax

load *file-url* [**overwrite** | **insert** | **append**]

Context

candidate

Description

This command loads a previously saved candidate configuration into the current candidate. The edit point is set to the end of the loaded configuration lines. The current candidate configuration cannot be modified while a load is in progress.

If the current candidate configuration is empty, this command loads the file into the candidate without requiring any of the optional parameters. If the current candidate is not empty, the user must specify **overwrite**, **insert**, or **append**.

Default

n/a

Parameters

file-url

> the directory and filename to load

overwrite

> discards the contents of the current candidate and replaces them with the contents of the file

insert

> inserts the contents of the file at the current edit point

append

> inserts the contents of the file at the end of the current candidate

quit

Syntax

quit

Context

candidate

Description

This command exits candidate edit mode. The contents of the current candidate configuration are not deleted and the user can continue editing them later.

Default

n/a

redo

Syntax

redo [*count*]

Context

candidate

Description

This command reapplies the changes to the candidate that were previously removed using the **undo** command. All **undo** or **redo** history is lost when the operator exits candidate edit mode.

The **redo** command is blocked if another user has made changes in a CLI branch that would be impacted during the redo operation.

Default

n/a

Parameters

count

specifies the number of previous changes to reapply

> **Values**   1 to 50
>
> **Default**   1

replace

Syntax

replace [*line*]

Context

candidate

Description

This command displays the specified line (a single line only) and allows it to be changed.

Line numbers can be displayed with the **candidate view** command.

Default

edit-point

Parameters

line

specifies the line to replace

> **Values**   *line* | *offset* | **first** | **edit-point** | **last**
>
> *line* — the absolute line number
>
> *offset* — the line relative to the current edit point, prefixed with either +
> or - to indicate before or after the current edit point
>
> **first** — keyword to indicate the first line
>
> **edit-point** — keyword to indicate the current edit point
>
> **last** — keyword to indicate the last line that is not "exit"

save

Syntax

save *file-url*

Context

candidate

Description

This command saves the current candidate configuration to a file.

Default

n/a

Parameters

file-url

specifies the directory and filename

undo

Syntax

undo [*count*]

Context

candidate

Description

This command removes the most recent changes done to the candidate. The changes can be reapplied using the **redo** command. The **undo** and **redo** history is lost when the operator exits candidate edit mode. This command cannot be used to recover a candidate that has been discarded with a **candidate discard** command.

This command is blocked if another user has made changes in any of the CLI branches that would be impacted during the undo operation.

Default

1

Parameters

count

specifies the number of previous changes to remove

view

Syntax

view [*line*]

Context

candidate

Description

This command displays the candidate configuration along with line numbers that can be used for editing the candidate configuration.

Default

edit-point

Parameters

line

displays the candidate configuration starting at the specified point

Values   *line* | *offset* | **first** | **edit-point** | **last**

line — the absolute line number

offset — the line relative to the current edit point, prefixed with either + or - to indicate before or after the current edit point

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not "exit"

management

Syntax

management cli

Context

config>system

Description

This command enables the CLI management context.

Parameters

cli

specifies the management context

configuration

Syntax

configuration

Context

config>system>management

Description

This command enables the CLI management configuration context.

immediate

Syntax

[no] immediate

Context

config>system>management>configuration

Description

This command controls whether CLI commands in the **configure** context can make changes to the running configuration.

If the command is enabled, any configuration changes are immediately applied to the running configuration.

The **no** form of this command blocks configuration changes to the running configuration, and the user must use **candidate edit** mode to modify the configuration.

Default

immediate

3.11.2.4 Rollback commands

rollback

Syntax

rollback

Context

admin

config>system

Description

This command enables the context to configure rollback command parameters.

Default

n/a

compare

Syntax

compare [**to** *source2*]

compare *source1* **to** *source2*

Context

admin

admin>rollback

config>xx (where xx is any sub-branch at any level below config, but not at the config context itself)

Description

This command compares two configuration files. If the **compare** command is entered with no parameters defined, it compares the active configuration to the most recent rollback file. If the command is entered with the **source2** parameter defined, it compares the active configuration to the specified file. If the command is entered with both source parameters defined, it compares the first specified file to the second specified file.

> **Note:** In the CLI, the **source1** and **source2** parameters are called **checkpoint1** and **checkpoint2** in the **admin>rollback** context for this command. For simplicity, this command description uses **source1** and **source2** for all contexts.

The **compare** command with no parameters can only be used in the **admin>rollback** context. The **compare to source2** command can only be used in the **admin>rollback** or **config>**xx context. In the **admin** context, both source parameters must be specified.

> **Caution:** A compare operation does not check authorization of each line of output. Permission to execute the **compare** command from the **admin** branch should only be granted to users who are allowed to view the entire system configuration.

The defaults for the source parameters are context-dependent and differ based on the branch in which the command is executed.

Default

admin context: no defaults (**source1** and **source2** must be specified)

admin>rollback context: *source1* = active-cfg, *source2* = latest-rb

config>*xx* context: *source1* = active-cfg, no default for *source2*

Parameters

source1, source2

the configuration files to compare

Values	active-cfg	the active operational system configuration
	rescue	the rollback rescue file from the configured rescue location
	latest-rb	the most recent rollback checkpoint file from the configured rollback location, with the suffix *.rb
	checkpoint-id	The ID value (*x*) of a specific rollback checkpoint file from the configured rollback location with the suffix *.rb.*x*.
		The default range is 1 to 9 but the maximum value depends on the local-max-checkpoints and remote-max-checkpoints configurations.

delete

Syntax

delete *checkpoint-rescue*

Context

admin>rollback

Description

This command deletes a rollback checkpoint file and decrements the suffix ID numbers of all older rollback checkpoint files.

If the **config>redundancy>rollback-sync** command is enabled, deleting a rollback checkpoint file also deletes the backup file and decrements the suffix ID numbers on the standby CSM.

Default

n/a

Parameters

checkpoint-rescue

identifies a rollback checkpoint or rescue file to delete

Values	rescue	the rollback rescue file from the configured rescue location
	latest-rb	the most recent rollback checkpoint file from the configured rollback location, with the suffix *.rb

checkpoint-id	The ID value (*x*) of a specific rollback checkpoint file from the configured rollback location with the suffix *.rb.*x*.
	The default range is 1 to 9 but the maximum value depends on the local-max-checkpoints and remote-max-checkpoints configurations.

revert

Syntax

revert *checkpoint-rescue* [**now**]

Context

admin>rollback

Description

This command initiates a CLI configuration rollback revert operation that returns the configuration state of the node to a previously saved checkpoint file or rescue file. The rollback reversion minimizes impacts to running services. Configuration parameters that have changed since the last rollback checkpoint file was created, or items on which changed configurations have dependencies, are first reset to their default values and then restored to their previous values from the rollback checkpoint file.

Performing a configuration reversion can be briefly service-impacting in changed areas. There are no service impacts to configuration areas that did not change since the rollback checkpoint file was created.

Default

n/a

Parameters

checkpoint-rescue

identifies the rollback checkpoint or rescue file to revert to

Values	rescue	the rollback rescue file from the configured rescue location
	latest-rb	the most recent rollback checkpoint file from the configured rollback location, with the suffix *.rb
	checkpoint-id	The ID value (*x*) of a specific rollback checkpoint file from the configured rollback location with the suffix *.rb.*x*.
		The default range is 1 to 9 but the maximum value depends on the local-max-checkpoints and remote-max-checkpoints configurations.

now

forces a rollback reversion without prompting for confirmation

save

Syntax

save [**comment** *comment*] [**rescue**]

Context

admin>rollback

Description

This command saves the current operational configuration as a rollback checkpoint file at the configured rollback location, using the filename specified by the rollback-location command, with the suffix *.rb. The suffixes of all previously saved rollback checkpoint files are automatically incremented by one (*.rb becomes *.rb.1, *.rb.1 becomes *.rb.2, and so on).

By default, there can be a maximum of 10 rollback checkpoint files, the latest with suffix *.rb and nine older files with suffixes *.rb.1 through *.rb.9. If the maximum number of checkpoint files is reached and a new one is saved, the oldest checkpoint file is deleted. The maximum number of rollback checkpoint files that can be saved can be configured with the local-max-checkpoints and remote-max-checkpoints commands.

If the **rescue** keyword is used, this command saves the current operational configuration as a rescue rollback file at the location and with the filename specified by the rescue-location command. The rescue file uses the suffix *.rc. There can be only one rescue file saved at a time. Saving a new rescue file deletes and replaces any existing rescue file.

A valid rollback checkpoint and rescue location must be configured with the rollback-location and rescue-location commands before saving a checkpoint or rescue file.

Default

n/a

Parameters

comment

a string up to 255 characters in length describing the associated rollback checkpoint file

rescue

saves the current operational configuration as a rollback rescue file with the suffix *.rc

view

Syntax

view [*checkpoint-rescue*]

Context

admin>rollback

Description

This command displays the configuration settings saved in a rollback checkpoint or rescue file, or the active operational system configuration.

Default

latest-rb

Parameters

checkpoint-rescue

    identifies the configuration file to view

Values		
	rescue	the rollback rescue file from the configured rescue location
	latest-rb	the most recent rollback checkpoint file from the configured rollback location, with the suffix *.rb
	checkpoint-id	The ID value (*x*) of a specific rollback checkpoint file from the configured rollback location with the suffix *.rb.*x*.
		The default range is 1 to 9 but the maximum value depends on the local-max-checkpoints and remote-max-checkpoints configurations.

local-max-checkpoints

Syntax

local-max-checkpoints [*number*]

no local-max-checkpoints

Context

config>system>rollback

Description

This command configures the maximum number of rollback checkpoint files that can be saved to the local compact flash.

When the maximum number of files are saved, the oldest rollback checkpoint file has an ID value one less than the configured maximum, because one rollback checkpoint file is always the latest file and does not have an ID number. For example, if you configure the maximum number of checkpoints as 50, after performing 50 rollback **save** commands, there is a rollback checkpoint file with extension *.rb, and 49 older files with extension *.rb.1 to *.rb.49.

The **no** form of this command resets the maximum value to the default.

Default

10

Parameters

number

the maximum number of rollback checkpoint files

Values 1 to 50

remote-max-checkpoints

Syntax

remote-max-checkpoints [*number*]

no remote-max-checkpoints

Context

config>system>rollback

Description

This command configures the maximum number of rollback checkpoint files that can be saved on a remote device.

When the maximum number of files are saved, the oldest rollback checkpoint file has an ID value one less than the configured maximum, because one rollback checkpoint file is always the latest file and does not have an ID number. For example, if you configure the maximum number of checkpoints as 50, after performing 50 rollback **save** commands, there is a latest rollback checkpoint file with extension *.rb, and 49 older files with extension *.rb.1 to *.rb.49.

The **no** form of this command resets the maximum value to the default.

Default

10

Parameters

number

the maximum number of rollback checkpoint files

Values 1 to 200

rescue-location

Syntax

[**no**] **rescue-location** *file-url* | *rescue filename*

Context

config>system>rollback

Description

This command configures the location and generic filename of the rollback rescue configuration file.

A rescue file can be saved locally on the compact flash or on a remote device. The file URL must not include a filename extension. The suffix for the rollback rescue configuration file is *.rc and is automatically appended when the file is saved.

A valid rollback rescue location must be configured before a rollback save command is executed.

Default

no rescue-location

Parameters

file-url

the local or remote file path for the rollback rescue configuration file (see Table 14: URL types and syntax for parameter descriptions)

rescue filename

the generic filename for rollback rescue configuration files

rollback-location

Syntax

[**no**] **rollback-location** *file-url* | *rollback filename*

Context

config>system>rollback

Description

This command configures the location and generic filename of rollback checkpoint files. Files can be saved locally on the compact flash or on a remote device.

The *file-url* or *filename* must not include a filename extension. The suffixes for rollback checkpoint files are *.rb and *.rb.1 to *.rb.*x*, and are automatically appended when the file is saved.

A valid rollback checkpoint location must be configured before a rollback save command is executed.

Default

no rollback-location

Parameters

file-url

the local or remote file path for rollback checkpoint files (see Table 14: URL types and syntax for parameter descriptions)

Values		
	local-url	[*cflash-id*/][*file-path*] 200 chars max, including cflash-id directory length 99 chars max each
	remote-url	[{ftp://}*login*:*pswd*@ *remote-locn*/][*file-path*]
		255 chars max directory length 99 chars max each
	remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0..FFFF]H
		d - [0..255]D
		interface: the interface name, 32 chars max, mandatory for link local addresses
	cflash-id	cf3:|cf3-A:|cf3-B:

rollback filename

the generic filename for rollback checkpoint files

rollback-sync

Syntax

rollback-sync

Context

admin>redundancy

Description

This command copies all existing rollback checkpoint files from the active CSM compact flash to the standby CSM compact flash on a 7705 SAR-8 Shelf V2 or 7705 SAR-18. You can also enable the system to save an automatic backup of each new rollback checkpoint file with the command in the **config>redundancy** context.

Rollback checkpoint files can only be backed up from local sources and only by using the two dedicated **rollback-sync** commands. The **synchronize** commands in the **config>redundancy** and **admin>redundancy** contexts do not apply to rollback checkpoint files.

Default

n/a

rollback-sync

Syntax

[**no**] **rollback-sync**

Context

config>redundancy

Description

This command enables automatic synchronization of locally saved rollback checkpoint files between the active CSM and standby CSM.

When automatic rollback synchronization is enabled, a rollback **save** causes the new checkpoint file to be saved on both the active and standby CSMs if the rollback location is a local location. The suffixes of all older checkpoint files on both active and standby CSMs are incremented by one. Automatic synchronization only causes new rollback checkpoint files to be copied to both CSMs. Any rollback checkpoint files that were created before **rollback-sync** was enabled are not copied to the standby CSM. You can manually back up all files using the command in the **admin>redundancy** context.

Rollback checkpoint files can only be backed up from local sources and only by using the two dedicated **rollback-sync** commands. The **synchronize** commands in the **config>redundancy** and **admin>redundancy** contexts do not apply to rollback checkpoint files.

The **no** form of this command disables automatic synchronization of new rollback checkpoint files.

Default

no rollback-sync

3.11.2.5 Show commands

> **Note:** The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

alias

Syntax

alias

Context

show

Description

This command displays a list of existing aliases.

Output

The following output is an example of alias information, and Table 12: Alias field descriptions describes the fields.

Output example

```
ALU-103>config>system# show alias
===============================================================================
Alias-Name                    Alias-command-name
===============================================================================
sri                           show router interface
sse                           show service service-using cpipe
ssvll                         show service service-using vll
-------------------------------------------------------------------------------
Number of aliases : 3
===============================================================================
ALU-103>config>system#
```

Table 12: Alias field descriptions

Label	Description
Alias-Name	Displays the name of the alias
Alias-command-name	The command and parameter syntax that define the alias
Number of aliases	The total number of aliases configured on the router

candidate

Syntax

candidate

Context

show>system

Description

This command shows candidate configuration information.

Default

n/a

Output

The following output is an example of candidate information, and Table 13: Candidate configuration field descriptions describes the output fields.

Output example

```
*A:Sar8 Dut-A# show system candidate
===============================================================================
Candidate Config Information
===============================================================================
Candidate configuration state        : modified
Num editors/viewers                  : 1
Candidate cfg exclusive locked       : no
Last commit state                    : success
Last commit time                     : 2021/04/08 21:13:00
Last commit initiated user           : admin
Checkpoint created with last commit  : yes
Scheduled revert time                : N/A
Last commit revert time              : N/A
===============================================================================
Users in edit-cfg mode
===============================================================================
Username Type (from)
===============================================================================
admin Telnet (192.0.2.239)
===============================================================================
*A:Sar8 Dut-A#
```

Table 13: Candidate configuration field descriptions

Label	Description
Candidate configuration state	empty — there are no uncommitted changes in the candidate configuration
	modified — there are uncommitted changes in the candidate configuration
	unconfirmed — there are no uncommitted changes in the candidate configuration but the result of the last commit automatically reverts to a previous configuration unless it is confirmed before the timeout expires
Num editors/viewers	The number of CLI sessions currently in candidate edit mode
Candidate cfg exclusive locked	Indicates if a user has exclusively locked the candidate configuration using the **candidate edit exclusive** command
Last commit state	none — there have been no commits since the last reboot of the node
	in-progress — the system is currently committing the candidate configuration
	success — the last commit finished successfully
	revert-pending — the last commit finished successfully but has not been confirmed yet and an auto-revert will occur if it is not confirmed before the timeout expires
	failed — the last commit failed and has been undone

Label	Description
	revert-in-progress — the last commit finished successfully but was not confirmed in time and the system is currently reverting to a previous configuration
	reverted — the last commit finished successfully but was not confirmed in time and the system has reverted to a previous configuration
	revert-failed — the last commit finished successfully but was not confirmed in time and the system attempted a reversion but failed
Last commit time	The time at which the last commit attempt was started
Last commit initiated user	The name of the user who initiated the last candidate commit
Checkpoint created with last commit	Indicates if a rollback checkpoint was created after the previous commit completed
Scheduled revert time	The currently scheduled auto-revert time if the **confirmed** option is being used with a candidate commit
Last commit revert time	The time the system was last reverted to a previous configuration
Users in edit-cfg mode	Lists all the user sessions that are currently in candidate edit mode
Username	The name of the user that is currently in candidate edit mode
Type (from)	The type of session (such as console or Telnet) and the source of the session (such as the source IP address of the remote host)

4 File system management

This chapter provides information about file system management.

Topics in this chapter include:

- The file system
- Common configuration tasks
- File system command reference

4.1 The file system

The 7705 SAR file system is used to store files used and generated by the system; for example, image files, configuration files, logging files, and accounting files.

The **file** commands allow you to copy, create, move, and delete files and directories, navigate to a different directory, and display file or directory contents and the image version.

4.1.1 Compact flash device

The file system is based on a DOS file system. On the 7705 SAR, each CSM has an integrated compact flash device. The names for these devices are:

- cf3:
- cf3-A:
- cf3-B:

The first device name above (cf3:) is a relative device name in that it refers to the device local to the control processor on the CSM running the current console session. As in the DOS file system, the colon (":") at the end of the name indicates that it is a device.

The second and third device names (cf3-A: and cf3-B:) are absolute device names that refer directly to the device on CSM A or CSM B (CSM B applies only to chassis with redundant CSMs).

The device cf3-B: does not apply to the following chassis because they do not have redundant CSMs:

- 7705 SAR-A
- 7705 SAR-Ax
- 7705 SAR-M
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-Wx
- 7705 SAR-X

> **Note:**
> - The 7705 SAR-8 Shelf V2, 7705 SAR-18, 7705 SAR-H, and 7705 SAR-M have removable compact flash cards.
> - The 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Hc, and 7705 SAR-Wx do not have removable compact flash cards; they are shipped with integrated memory that is used to store system boot software, OS software, and configuration files and logs.
> - The 7705 SAR-X has two removable compact flash cards but they are not field-replaceable. Replacement of the devices is done as a repair service.

On the 7705 SAR-18, cf3: is used to store the software image required for system startup and operation, including the application load. The 7705 SAR-18 CSM also has two optional compact flash slots for two compact flash devices (cf1: and cf2:). These compact flash devices are also referred to as cf1-A:/cf1-B: and cf2-A:/cf2-B: to indicate whether they are on CSM A or CSM B. All the compact flash devices can be used to store software upgrades, statistics, logging files, accounting files, scripts, and configuration data.

> **Note:** To prevent corruption of open files in the file system, compact flashes should be removed on those chassis that have replaceable compact flash cards only when the CFs are administratively shut down. The 7705 SAR gracefully closes any open files on the device so that it can be safely removed.

4.1.2 URLs

The arguments for the 7705 SAR file commands are modeled after the standard universal resource locator (URL).

A URL can refer to a file (a *file-url*) or a directory (a *directory-url*).

The 7705 SAR supports operations on both the local file system and on remote files. For the purposes of categorizing the applicability of commands to local and remote file operations, URLs are divided into three types of URLs: local, FTP, and TFTP

The syntax for each of the URL types is listed in the following table.

Table 14: URL types and syntax

URL type	Syntax	Notes
local-url	[*cflash-id/*] [*file-path*]	*cflash-id* is the compact flash device name
		Values: cf1: | cf1-A: | cf1-B: | cf2: | cf2-A: | cf2-B: | cf3: | cf3-A: | cf3-B:
		(the 7705 SAR-18 supports all values; the 7705 SAR-8 Shelf V2 supports cf3:, cf3-A:., and cf3-B:; all fixed platforms support cf3: and cf3-A:)
		Length: 200 characters maximum, including *cflash-id*; directory length is 99 characters maximum each
		file-path is the path to the directory or file
remote-url	[**ftp**://*login*:*pswd*@*remote-locn/*] [*file-path*]	An absolute FTP path from the root of the remote file system:

URL type	Syntax	Notes
		Length: 255 characters maximum (could be less depending on command); directory length is 99 characters maximum each
		login is the FTP username
		pswd is the FTP user password
		remote-locn is the remote host (hostname or IP address) Values: • *hostname*: hostname of the remote location, up to 128 characters maximum • *ipv4-address*: a.b.c.d • "["*ipv6-address*"]" (address must be enclosed in square brackets) – x:x:x:x:x:x:x:x[-*interface*] – x:x:x:x:x:x:d.d.d.d[-*interface*] – x: [0 to FFFF]H – d: [0 to 255]D – *interface:* the interface name, 32 characters maximum, mandatory for link local addresses
		file-path is the path to the directory or file
	ftp:///*login*:*pswd*]**@**host**l.l** path	A relative FTP path from the user's home directory. Note the period and slash ("./") in this syntax, as compared to the absolute path.
destination-file-url	[*user@hostname:file-path*]	The destination file to be copied to a remote host file system
		user is the SSH user, 32 characters maximum
		hostname is the hostname of the remote location, up to 128 characters maximum Values: • *dns-name*: 128 characters maximum • *ipv4-address*: a.b.c.d • "["*ipv6-address*"]" (address must be enclosed in square brackets) – x:x:x:x:x:x:x:x[-*interface*] – x:x:x:x:x:x:d.d.d.d[-*interface*] – x: [0 to FFFF]H – d: [0 to 255]D

URL type	Syntax	Notes
		– *interface:* the interface name, 32 characters maximum, mandatory for link local addresses
		file-path is the destination file path, 200 characters maximum; directory length is 99 characters maximum each
tftp-url	**tftp**://*login:pswd@remote-locn*/*file-path*	TFTP is only supported for operations on file-urls

Table 15: File command local and remote file system support lists the commands that are supported both locally and remotely.

Table 15: File command local and remote file system support

Command	local-url	ftp-url	tftp-url
attrib	✓		
cd	✓	✓	
copy	✓	✓	✓
delete	✓	✓	
dir	✓	✓	
md		✓	
move	✓	✓	
rd		✓	
repair			
scp	source only		
type	✓	✓	✓
version	✓	✓	✓

The 7705 SAR accepts either forward slash ("/") or backslash ("\") characters to delimit directory and/ or filenames in URLs. Similarly, the 7705 SAR SCP client application uses either slash or backslash characters, but not all SCP clients treat backslash characters as equivalent to slash characters. In particular, UNIX systems interpret the backslash character as an "escape" character. This causes problems when using an external SCP client application to send files to the 7705 SAR SCP server. If the external system treats the backslash like an escape character, the backslash delimiter gets stripped by the parser and is not transmitted to the 7705 SAR SCP server.

For example, a destination directory specified as "cf3:\dir1\file1" is transmitted to the 7705 SAR SCP server as "cf3:dir1file1" where the backslash escape characters are stripped by the SCP client system

before transmission. On systems where the client treats the backslash like an "escape" character, a double backslash "\\" or the forward slash "/" can typically be used to properly delimit directories and the filename.

4.1.3 Wildcards

The 7705 SAR supports the standard DOS wildcard characters. The asterisk (*) can represent zero or more characters in a string of characters, and the question mark (?) can represent any one character.

Example:

```
ALU-1>file cf3:\ # copy test*.cfg siliconvalley
    cf3:\testfile.cfg
    1 file(s) copied.
    ALU-1>file cf3:\ # cd siliconvalley
    ALU-1>file cf3:\siliconvalley\ # dir
     Volume in drive cf3 on slot A has no label.
    Directory of cf3:\siliconvalley\
    05/10/2006 11:32p      <DIR>            .
    05/10/2006 11:14p      <DIR>            ..
    05/10/2006 11:32p                  7597 testfile.cfg
         1 File(s)                     7597 bytes.
         2 Dir(s)                   1082368 bytes free.
    ALU-1>file cf3:\siliconvalley\ #
```

As in a DOS file system, the 7705 SAR wildcard characters can only be used in some of the file commands.

4.2 Common configuration tasks

The following sections describe the basic system tasks that can be performed.

- Modifying file attributes
- Creating and navigating directories
- Copying files
- Moving files
- Deleting files and removing directories
- Displaying directory and file information
- Repairing the file system

> **Note:** When a file system operation is performed with a command that can potentially delete or overwrite a file system entry (such as a **copy**, **delete**, **move**, **rd**, or **scp** command), a prompt appears to confirm the action. The **force** keyword performs the copy, delete, move, rd, or scp action without displaying the confirmation prompt.

4.2.1 Modifying file attributes

The system administrator can change the read-only attribute in the local file. Enter the **attrib** command with no options to display the contents of the directory and the file attributes.

Use the CLI syntax displayed below to modify file attributes:

CLI Syntax:
```
file>
    attrib [+r | -r] file-url
```

The following displays an example of the command syntax:

Example:
```
# file
file cf3:\ # attrib
file cf3:\ # attrib +r BOF.SAV
file cf3:\ # attrib
```

The following displays the file configuration:

```
     ALU-1>file cf3:\ # attrib
     cf3:\bootlog.txt
     cf3:\bof.cfg
     cf3:\boot.ldr
     cf3:\bootlog_prev.txt
     cf3:\BOF.SAV
 ALU-1>file cf3:\ # attrib +r BOF.SAV
     ALU-1>file cf3:\ # attrib
     cf3:\bootlog.txt
     cf3:\bof.cfg
     cf3:\boot.ldr
     cf3:\bootlog_prev.txt
     R cf3:\BOF.SAV
```

4.2.2 Creating and navigating directories

Use the **md** command to create a new directory in the local file system, one level at a time.

Use the **cd** command to navigate to different directories.

Use the CLI syntax displayed below to create a new directory:

CLI Syntax:
```
file>
    md file-url
```

The following displays an example of the command syntax:

Example:
```
file cf3:\ # md test1
file cf3:\ # cd test1
file cf3:\test1\ # md test2
file cf3:\test1\ # cd test2
file cf3:\test1\test2\ # md test3
file cf3:\test1\test2\ # cd test3
file cf3:\test1\test2\test3 #
```

4.2.3 Copying files

Use the **copy** command to upload or download an image file, configuration file, or other file types to or from a flash card or a TFTP server.

The **scp** command copies files between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH.

The source file for the **scp** command must be local. The file must reside on the 7705 SAR router. The destination file must be in the format: user@host:file-name. The destination does not need to be local.

Use the CLI syntax displayed below to copy files:

CLI syntax:
```
file>
    copy source-file-url dest-file-url [force]
    scp local-file-url destination-file-url [router router name | service-id] [force]
```

The following displays an example of the **copy** command syntax:

Example:
```
ALU-1>file cf3::\ # copy 104.cfg cf3::\test1\test2\test3\test.cfg
ALU-1>file cf3::\ # scp file1 admin@192.168.x.x:cf3::\file1
ALU-1>file cf3::\ # scp file2 user2@192.168.x.x:/user2/file2
ALU-1>file cf3::\ # scp cf3::/file3 admin@192.168.x.x:cf3::\file3
```

4.2.4 Moving files

Use the **move** command to move a file or directory from one location to another.

Use the CLI syntax displayed below to move files:

CLI Syntax:
```
file>
    move old-file-url new-file-url [force]
```

The following displays an example of the command syntax:

Example:
```
ALU-1>file cf3::\test1\test2\test3\ # move test.cfg cf3::\test1
     cf3::\test1\test2\test3\test.cfg
ALU-1>file cf3::\test1\test2\test3\ # cd ..
ALU-1>file cf3::\test1\test2\ # cd ..
ALU-1>file cf3::\test1\ # dir

 Directory of cf3::\test1\
     05/04/2006 07:58a      <DIR>              .
     05/04/2006 07:06a      <DIR>              ..
     05/04/2006 07:06a      <DIR>              test2
     05/04/2006 07:58a              25278 test.cfg
      1 File(s)                   25278 bytes.
      3 Dir(s)                  1056256 bytes free.
 ALU-1>file cf3::\test1\ #
```

4.2.5 Deleting files and removing directories

Use the **delete** and **rd** commands to delete files and remove directories. Directories can be removed even if they contain files and/or subdirectories. To remove a directory that contains files or subdirectories or both, use the **rd rf** command. When files or directories are deleted, they cannot be recovered.

The **force** option deletes the file or directory without prompting the user to confirm.

Use the CLI syntax displayed below to delete files and then remove directories:

CLI syntax:
```
file>
    delete file-url [force]
    rd file-url [force]
```

The following displays an example of the command syntax:

```
ALU-1>file cf3::\test1\ # delete test.cfg
ALU-1>file cf3::\test1\ # delete abc.cfg
ALU-1>file cf3::\test1\test2\ # cd test3
ALU-1>file cf3::\test1\test2\test3\ # cd ..
ALU-1>file cf3::\test1\test2\ # rd test3
ALU-1>file cf3::\test1\test2\ # cd ..
ALU-1>file cf3::\test1\ # rd test2
ALU-1>file cf3::\test1\ # cd ..
ALU-1>file cf3::\ # rd test1
ALU-1>file cf3::\ #
```

Use the CLI syntax displayed below to remove a directory without first deleting files or subdirectories:

CLI syntax:
```
file>
    rd file-url rf
```

4.2.6 Displaying directory and file information

Use the **dir** command to display a list of files on a file system.

Use the **type** command to display the contents of a file.

Use the **version** command to display the version of a 7705 SAR both.tim file.

Use the CLI syntax displayed below to display directory and file information:

CLI syntax:
```
file>
    dir [file-url]
    type file-url
    version file-url
```

The following displays an example of the command syntax:

```
A:ALU-1# file
A:ALU-1>file cf3::\ # dir

 Volume in drive cf3: on slot A has no label.

 Volume in drive cf3: on slot A is formatted as FAT32.
```

```
Directory of cf3::\

02/08/2008  11:23a              140584 boot.ldr
02/07/2008  12:19p                 786 bof.cfg
02/13/2008  05:42p                2058 bootlog.txt
01/13/2008  05:42p                2434 bootlog_pre.txt
01/30/2008  05:17p                 797 bof.cfg.arash
01/25/2008  04:11p     <DIR>           TXT
01/30/2008  11:36a                 787 bof.cfg.ftp
01/30/2008  01:11p                 736 bof.cfg.root
01/30/2008  11:35a                 886 bof.cfg.deep
01/30/2008  11:35a                 483 bof.cfg.JC
               8 File(s)              411097 bytes.
               1 Dir(s)             1043456 bytes free.
A:ALU-1>file cf3::\ # type bof.cfg
# TiMOS-B-1.1.R1 both/hops NOKIA SAR 7705
# Copyright (c) 2016 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Wed Apr 9 09:53:01 EDT 2016 by csabuild in /rel2.0/b1/R1/panos/main

# Generated WED APR 09 20:18:06 2016 UTC

    primary-image    ftp://*:*@xxx.xxx.xxx.xx/home/csahwreg17/images/both.tim
    primary-config   ftp://*:*@ xxx.xxx.xxx.xx /home/csahwreg17/images/dut-a.cfg
    address          xxx.xxx.xxx.xx /24 active
    address          xxx.xxx.xxx.xx /24 standby
    primary-dns      xxx.xxx.xxx.xx
    dns-domain       labs.ca.alcatel-lucent.com
    static-route     xxx.xxx.0.0/16 next-hop xxx.xxx.xxx.x
    autonegotiate
    duplex           full
    speed            100
    wait             3
    persist          off
    console-speed    115200

A:ALU-1>file cf3::\ #
```

4.2.7 Repairing the file system

Use the **repair** command to check a compact flash device for errors and repair any errors found.

Use the CLI syntax displayed below to check and repair a compact flash device:

CLI syntax:
```
file
    repair [flash-id]
```

The following displays an example of the command syntax:

```
ALU-1>file cf3:\ # repair
Checking drive cf3: on slot A for errors...
Drive cf3: on slot A is OK.
```

4.3 File system command reference

4.3.1 Command hierarchy

4.3.1.1 Configuration commands

```
file
    - attrib [+r | -r] file-url
    - attrib
    - cd [file-url]
    - copy source-file-url dest-file-url [force]
    - delete file-url [force]
    - dir [file-url] [sort-order {d | n | s}] [reverse]
    - format [flash-id] [reliable]
    - md file-url
    - move old-file-url new-file-url [force]
    - rd file-url rf
    - rd file-url [force]
    - repair [flash-id]
    - scp local-file-url destination-file-url [router router-instance] [force]
    - scp local-file-url destination-file-url [service service-name] [force]
    - [no] shutdown [active] [standby]
    - [no] shutdown flash-id
    - type file-url
    - version file-url [check]
```

4.3.2 Command descriptions

- [Configuration commands](#)

4.3.2.1 Configuration commands

file

Syntax

file

Context

root

Description

This command enters the context to perform file system operations.

When entering the **file** context, the prompt changes to reflect the present working directory. Navigating the file system with the **cd ..** command results in a changed prompt.

The **exit all** command leaves the file system/file operation context and returns to the <ROOT> CLI context. The state of the present working directory is maintained for the CLI session. Entering the **file** command returns the cursor to the working directory where the **exit** command was issued.

attrib

Syntax

attrib [**+r** | **-r**] *file-url*

attrib

Context

file

Description

This command sets or clears/resets the read-only attribute for a file in the local file system.

To list all files and their current attributes, enter **attrib** or **attrib x** where **x** is either the filename or a wildcard (*).

When an **attrib** command is entered to list a specific file or all files in a directory, the file's attributes are displayed with or without an "R" preceding the filename. The "R" implies that the **+r** is set and that the file is read-only. Files without the "R" designation imply that the **-r** is set and that the file is read-write-all. For example:

```
ALU-1>file cf3:\ # attrib
```

```
                  cf3:\bootlog.txt
                  cf3:\bof.cfg
                  cf3:\boot.ldr
                  cf3:\sr1.cfg
                  cf3:\test
                  cf3:\bootlog_prev.txt
         R    cf3:\BOF.SAV
```

Parameters

file-url

the URL for the local file (see Table 14: URL types and syntax for parameter descriptions)

+r

sets the read-only attribute on the specified file

-r

clears/resets the read-only attribute on the specified file

cd

Syntax

cd [*file-url*]

Context

file

Description

This command displays or changes the current working directory in the local file system.

Parameters

file-url

the URL for the local file (see Table 14: URL types and syntax for parameter descriptions)

<none>

displays the current working directory

..

signifies the parent directory. This can be used in place of an actual directory name in a
directory-url.

directory-url

the destination directory

copy

Syntax

copy *source-file-url dest-file-url* [**force**]

Context

file

Description

This command copies a file or all files in a directory from a source URL to a destination URL. At least one of the specified URLs should be a local URL. The optional wildcard (*) can be used to copy multiple files that share a common (partial) prefix and/or (partial) suffix.

When a file is copied to a destination with the same filename, the original file is overwritten by the new file specified in the operation. The following prompt appears if the destination file already exists:

"Overwrite destination file (y/n)?"

For example:

To copy a file named srcfile in a directory called test on cf3: in slot CSM B to a file called destfile in a directory called production on cf3: in slot CSM A, the syntax is:

```
file cf3:\ # copy cf3-B:/test/srcfile cf3-A:/production/destfile
```

To FTP a file named 121201.cfg in directory mydir stored on cf3: in slot CSM A to a network FTP server with IP address 192.0.2.255 in a directory called backup with a destination filename of 121201.cfg, the FTP syntax is:

```
copy cf3-A:/mydir/121201.cfg 192.0.2.255.79/backup/121201.cfg
```

Parameters

source-file-url

the location of the source file or directory to be copied (see *file-url*)

dest-file-url

the destination of the copied file or directory (see *file-url*)

force

forces an immediate copy of the files without displaying a user prompt message

file-url

the local or remote URL (see Table 14: URL types and syntax for parameter descriptions)

delete

Syntax

delete *file-url* [**force**]

Context

file

Description

This command deletes the specified file.

The optional wildcard "*" can be used to delete multiple files that share a common (partial) prefix and/or (partial) suffix. When the wildcard is entered, the following prompt displays for each file that matches the wildcard:

"Delete file <filename> (y/n)?"

Parameters

file-url

the filename to delete (see Table 14: URL types and syntax for parameter descriptions)

force

forces an immediate deletion of the specified files

file delete * force deletes all the wildcard matching files without displaying a user prompt message

dir

Syntax

dir [*file-url*] [**sort-order** {**d** | **n** | **s**}] [**reverse**]

Context

file

Description

This command displays a list of files and subdirectories in a directory. The **sort-order** keyword sorts the files by date, name, or size. The default is to list in ascending order (oldest to newest, A to Z, or smallest to largest); to list the files in descending order, use the **reverse** keyword.

Parameters

file-url

the path or directory name (see Table 14: URL types and syntax for parameter descriptions)

Use *file-url* with the optional wildcard (*) to reduce the number of files to list.

Default   lists all files in the present working directory, sorted by name (in ascending order)

sort-order

specifies the order by which the files are sorted

Values   d – sorts by date

n – sorts by filename

s – sorts by file size

reverse

sorts the files in descending order

format

Syntax
format [*flash-id*] [**reliable**]

Context
file

Description
This command formats the compact flash. The compact flash must be shut down before formatting.

Parameters
cflash-id

the compact flash type (see Table 14: URL types and syntax for parameter descriptions and values)

reliable

enables the reliance file system and disables the default DOS file system. This option is valid only on compact flashes 1 and 2.

md

Syntax
md *file-url*

Context
file

Description
This command creates a new directory in a file system.

Directories can only be created one level at a time.

Parameters
file-url

the directory name to be created (see Table 14: URL types and syntax for parameter descriptions)

move

Syntax
move *old-file-url new-file-url* [**force**]

Context

file

Description

This command moves a local file, system file, or a directory. If the target already exists, the command fails and an error message displays.

The following prompt appears if the destination file already exists:

"Overwrite destination file (y/n)?"

Parameters

old-file-url

the file or directory to be moved (see Table 14: URL types and syntax for parameter descriptions)

new-file-url

the new destination to place the *old-file-url* (see Table 14: URL types and syntax for parameter descriptions)

force

forces an immediate move of the specified files

file move force executes the command without displaying a user prompt message

rd

Syntax

rd *file-url* **rf**

rd *file-url* [**force**]

Context

file

Description

This command removes (deletes) a directory in a file system.

If the directory is empty, the **rd** command is used to remove it. The **force** option executes the command without prompting the user to confirm the action.

If the directory contains files and/or subdirectories, the **rf** parameter must be used to remove the directory.

Parameters

file-url

the directory to be removed (see Table 14: URL types and syntax for parameter descriptions)

rf

forces a recursive delete (directory and its subdirectories/files)

force

>   forces an immediate deletion of the specified directory; no user prompt is displayed

repair

Syntax

repair [*flash-id*]

Context

file

Description

This command checks a compact flash device for errors and repairs any errors found.

Parameters

cflash-id

>   the compact flash slot ID to be shut down or enabled. When a specific *cflash-id* is
>   specified, then that drive is shut down. If no *cflash-id* is specified, the drive referred to by
>   the current working directory is assumed. If a slot number is not specified, then the active
>   CSM is assumed.

> >   **Values**   see Table 14: URL types and syntax for parameter descriptions and
> >   values

> >   **Default**   the current compact flash device

scp

Syntax

scp *local-file-url destination-file-url* [**router** *router-instance*] [**force**]

scp *local-file-url destination-file-url* [**service** *service-name*] [**force**]

Context

file

Description

This command copies a local file to a remote host file system. It uses **ssh** for data transfer, and uses the
same authentication and provides the same security as **ssh**. When the command is entered, the following
prompt appears:

"Are you sure (y/n)?"

The destination must specify a user and a host.

Parameters

local-file-url

the local source file or directory (see Table 14: URL types and syntax for parameter descriptions)

destination-file-url

the destination file (see Table 14: URL types and syntax for parameter descriptions)

router-instance

specifies the router name or service ID

Values	*router-name*: Base, management
	service-id: 1 to 2147483647
Default	Base

service-name

specifies the service name, 64 characters maximum

force

forces an immediate copy of the specified file

file scp *local-file-url destination-file-url* [**router** *router-instance* | **service-name** *service-name*] **force** executes the command without displaying a user prompt message

shutdown

Syntax

[**no**] **shutdown** [**active**] [**standby**]

[**no**] **shutdown** *flash-id*

Context

file

Description

This command shuts down (unmounts) the specified CSMs.

Use the **no shutdown** [**active**] [**standby**] command to enable one or both CSMs.

Use the **no shutdown** *flash-id* command to enable a compact flash (cf3: on all platforms; cf1: or cf2: on the 7705 SAR-18) on the CSM. The **no shutdown** command can be issued for a specific slot when no compact flash is present. When a compact flash is installed in the slot, the device is activated upon detection.

In redundant systems, use the **no shutdown** command on cf3: on both CSMs in order to facilitate synchronization. See the synchronize command in the **config>redundancy** context.

The **shutdown** command must be issued before removing a compact flash. If no parameters are specified, the drive referred to by the current working directory shuts down.

LED status indicators — the following states are possible for the compact flash:

Operational: If a compact flash is present in a drive and operational (**no shutdown**), the respective LED is lit green. The LED flickers when the compact flash is accessed. Do **not** remove the compact flash during a read/write operation.

State: admin = up, operational = up, equipped = yes

Flash defective: If a compact flash is defective, the respective LED blinks amber to reflect the error condition and a trap is raised.

State: admin = up/down, operational = faulty, equipped = no

Flash drive shut down: When the compact flash drive is shut down and a compact flash is present, the LED is lit amber. In this state, the compact flash can be ejected.

State: admin = down, operational = down, equipped = yes

No compact flash present, drive shut down: If no compact flash is present and the drive is shut down, the LED is unlit.

State: admin = down, operational = down, equipped = no

No compact flash present, drive enabled: If no compact flash is present and the drive is not shut down, the LED is unlit.

State: admin = up, operational = down, equipped = no

Ejecting a compact flash: The compact flash drive should be shut down before ejecting a compact flash. The LED should turn to solid (not blinking) amber. This is the only way to safely remove the compact flash. If a compact flash drive is not shut down before a compact flash is ejected, the LED blinks amber for approximately 5 s before shutting off.

State: admin = down, operational = down, equipped = yes

The **shutdown** or **no shutdown** state is not saved in the configuration file. Following a reboot, all compact flash drives are in their default state.

Default

no shutdown — compact flash device is administratively enabled

Parameters

cflash-id

the compact flash slot ID to be shut down or enabled. If a *cflash-id* is specified, the drive is shut down or enabled. If no *cflash-id* is specified, the drive referred to by the current working directory is assumed. If a slot number is not specified, the active CSM is assumed.

Values   see Table 14: URL types and syntax for parameter descriptions and values

active

all drives on the active CSM are shut down or enabled

standby

all drives on the standby CSM are shut down or enabled

If both **active** and **standby** keywords are specified, all drives on both CSMs are shut down or enabled.

type

Syntax

type file-url

Context

file

Description

This command displays the contents of a text file.

Parameters

file-url

the file contents to display (see Table 14: URL types and syntax for parameter
descriptions)

version

Syntax

version *file-url*[**check**]

Context

file

Description

This command displays the version of a -TiMOS both.tim file.

Parameters

file-url

the filename of the target file (see Table 14: URL types and syntax for parameter
descriptions)

check

validates the .tim file

Output

The following example shows the version of a -TiMOS both.tim file.

Output example

```
A:ALU-1# file version cf3:/both.tim
TiMOS-B-0.0.R1 for NOKIA SAR 7705
A:ALU-1# file version ftp://timos:timos@xxx.xxx.xx.xx/./both.tim check
Validation successful
TiMOS-I-0.0.R1 for NOKIA SAR 7705
```

```
B:Performance#
```

5 Boot options

This chapter provides information about configuring boot option parameters.

Topics in this chapter include:

- System initialization
- Initial system startup process overview
- Boot loader file protection
- Accessing the CLI
- Accessing MPT radios connected to a 7705 SAR
- Configuration notes
- Configuring the BOF with the CLI
- BOF command reference

5.1 System initialization

Depending on the chassis, the primary copy of 7705 SAR software is located either on a removable compact flash card that is shipped with the 7705 SAR router or in the router on-board flash memory. The compact flash (`cf3`) contains a copy of the 7705 SAR image, the bootstrap file (`boot.ldr`), and the boot options file (BOF). The compact flash can also be used to store configurations and executable images. These configurations and images can also be stored at an FTP file location.

The following chassis have removable compact flash cards:

- 7705 SAR-8 Shelf V2
- 7705 SAR-18
- 7705 SAR-H
- 7705 SAR-M

All other chassis have integrated memory that cannot be removed.

> **Note:** In most cases you must have a console connection to access the node when there is no network connectivity to the node. Some commands can be given to the node through the ACO/LT button before there is network connectivity. See Automatic Discovery Protocol. Also see the appropriate chassis installation guide, "Automatic Discovery Protocol".

Starting a 7705 SAR begins with hardware initialization (a reset or power cycle). By default, the system searches the compact flash (cf3) for the `boot.ldr` file (also known as the boot loader or bootstrap file). The `boot.ldr` file is the image that reads and executes the system initialization commands configured in the BOF. The default value to initially search for the `boot.ldr` file on cf3 cannot be modified.

If the system cannot load or cannot find the `boot.ldr` file on the compact flash memory device (cf3), the system reboots continuously in an attempt to successfully find and load the file. If this happens, the available options depend on the chassis.

For the 7705 SAR-8 Shelf V2 and 7705 SAR-18, there are two options:

- remove the compact flash, connect it to a PC, and download another software package from OLCS; contact your Nokia support representative for detailed instructions

- return the faulty CSM to Nokia for replacement

For the 7705 SAR-M, there are two options:

- remove the compact flash, connect it to a PC, and download another software package from OLCS; contact your Nokia support representative for detailed instructions

- return the faulty chassis to Nokia for replacement

For the 7705 SAR-H, there are one or two options:

- if the compact flash is accessible, connect it to a PC, and download another software package from OLCS; contact your Nokia support representative for detailed instructions

- return the faulty chassis to Nokia for replacement

For the 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Hc, 7705 SAR-Wx, and 7705 SAR-X, return the faulty chassis to Nokia for replacement.

When the bootstrap image is loaded, the BOF is read to obtain the location of the image and configuration files. The BOF should be located on the same compact flash drive as the `boot.ldr` file. If the BOF cannot be found or loaded, the system prompts the user for alternate software and configuration file locations.

The following example displays the output when the boot sequence is interrupted.

```
...
```

```
Hit a key within 3 seconds to change boot parms...
You must supply some required Boot Options. At any prompt, you can type:
   "restart" - restart the query mode.
   "reboot"  - reboot.
   "exit"    - boot with existing values.

Press ENTER to begin, or 'flash' to enter firmware update...

Software Location
-----------------
   You must enter the URL of the TiMOS software.
   The location can be on a Compact Flash device,
   or on the network.

   Here are some examples
      cf3:/timos2.0R1
      ftp://user:passwd@192.168.xx.xxx/./timos2.0R1
      tftp://192.168.xx.xxx/./timos2.0R1

The existing Image URL is 'ftp://*.*@192.168.xx.xxx/./rel/0.0/xx'
Press ENTER to keep it.
Software Image URL:
Using: 'ftp://*.*@192.168.xx.xxx/./rel/0.0/xx'

Configuration File Location
---------------------------
   You must enter the location of configuration
   file to be used by TiMOS. The file can be on
   a Compact Flash device, or on the network.

   Here are some examples
      cf1:/config.cfg
      ftp://user:passwd@192.168.xx.xxx/./config.cfg
```

```
        tftp://192.168.xx.xxx/./config.cfg

The existing Config URL is 'cf3:/config.cfg'
Press ENTER to keep it, or the word 'none' for no Config URL.
Config File URL:
Using: 'cf3:/config.cfg'

Network Configuration
---------------------
   You specified a network location for either the
   software or the configuration file. You need to
   assign an IP address for this system.

   The IP address should be entered in standard
   dotted decimal form with a network length.
        example:   192.168.xx.xxx/24
```

5.1.1 Display on non-redundant models

```
The existing IP address is 192.168.xx.xxx/20. Press ENTER to keep it.
Enter IP Address:
Using: 192.168.xx.xxx/20
```

5.1.2 Display on redundant models

```
The existing Active IP address is 192.168.xx.xxx/20. Press ENTER to keep it.
Enter Active IP Address:
Using: 192.168.xx.xxx/20

The existing Standby IP address is 192.168.xx.xxx/20. Press ENTER to keep it.
Enter Standby IP Address (Type 0 if none desired):
Using: 192.168.xx.xxx/20


Would you like to add a static route? (yes/no) y

Static Routes
-------------
   You specified network locations which require
   static routes to reach. You will be asked to
   enter static routes until all the locations become
   reachable.

   Static routes should be entered in the following format:
   prefix/mask next-hop ip-address
        example:     192.168.xx.xxx/16 next-hop 192.168.xx.xxx

Enter route: 1.x.x.0/24 next-hop 192.168.xx.xxx
OK

Would you like to add another static route? (yes/no) n

New Settings
------------
    primary-image    ftp://*.*@192.168.xx.xx/./rel/0.0/xx
    primary-config   cf3:/config.cfg
```

```
      address         192.168.xx.xx/20 active
      primary-dns     192.168.xx.xx
      dns-domain      xxx.xxx.com
      static-route    1.x.x.0/24 next-hop 192.168.xx.xxx
      autonegotiate
      duplex          full
      speed           100
      wait            3
      persist         off

Do you want to overwrite cf3:/bof.cfg with the new settings? (yes/no): y

Successfully saved the new settings in cf3:/bof.cfg
```

Figure 4: System initialization - part 1 displays the system initialization sequence.

Figure 4: System initialization - part 1
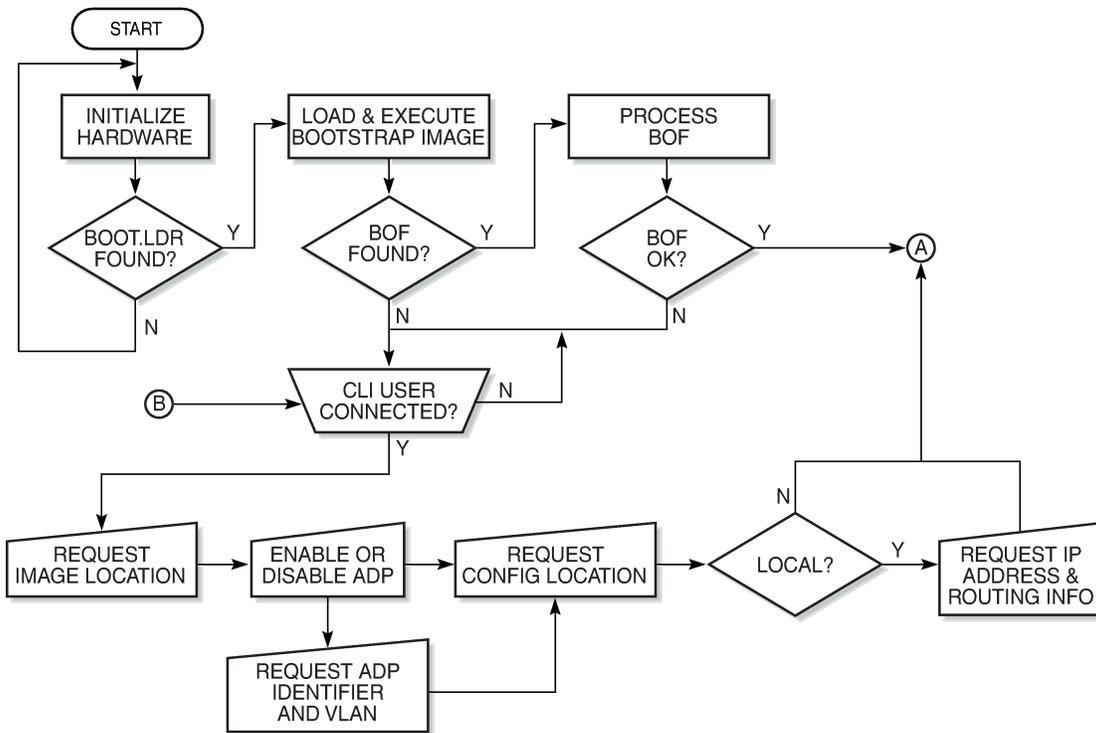
Figure 5: Files on the compact flash displays the compact flash directory structure and filenames.

Figure 5: Files on the compact flash
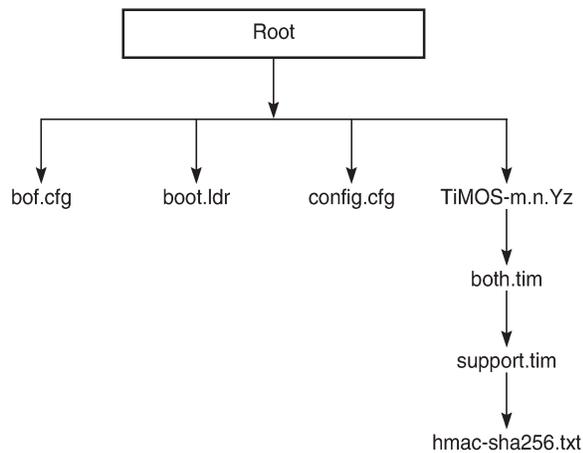
Files on the compact flash are:

- bof.cfg — boot options file
- boot.ldr — bootstrap image
- config.cfg — default configuration file
- TiMOS-m.n.Yz:

    m — major release number

    n — minor release number

    Y: type of release

    – A — Alpha release
    – B — Beta release
    – M — maintenance release
    – R — released software

    z — version number

    – both.tim — CSM image file
    – support.tim — field-programmable gate array (FPGA) file
    – hmac-sha256.txt

> **Note:**
> - The support.tim file is included in the software bundles for the following platforms only: 7705 SAR-8 Shelf V2, 7705 SAR-18, 7705 SAR-H, 7705 SAR-M, and 7705 SAR-X.
> - The hmac-sha256.txt file is supported in FIPS-140-2 mode only. See FIPS-140-2 mode for more information.

5.1.3 Configuration and image loading

When the system executes the `boot.ldr` file, the initialization parameters from the BOF are processed. Three locations can be configured for the system to search for the files that contain the runtime image. The locations can be local or remote. The first location searched is the primary image location. If not found, the secondary image location is searched, and lastly, the tertiary image location is searched.

If the files cannot be found or loaded, the system enters a console message dialog session prompting the user to enter alternate file locations and filenames.

When the runtime image is successfully loaded, control is passed from the bootstrap loader to the image. Depending on the options in the BOF file, the runtime image loads the configuration in one of two ways.

If ADP is enabled, no configuration files are processed at startup. Instead, ADP discovers the node configuration from the network and the `primary-config` file is generated based on the configuration discovered by ADP. Any existing `primary-config` file is backed up, then overwritten.

If ADP is not enabled, the runtime image attempts to locate the configuration file as configured in the BOF. Like the runtime image, three locations can be configured for the system to search for the configuration file. The locations can be local or remote. The first location searched is the primary configuration location. If not found, the secondary configuration location is searched, and lastly, the tertiary configuration location is searched.

The configuration file includes chassis, CSM, adapter card and port configurations, as well as system, routing, and service configurations.

Figure 6: System initialization - part 2 displays the boot sequence.

Figure 6: System initialization - part 2
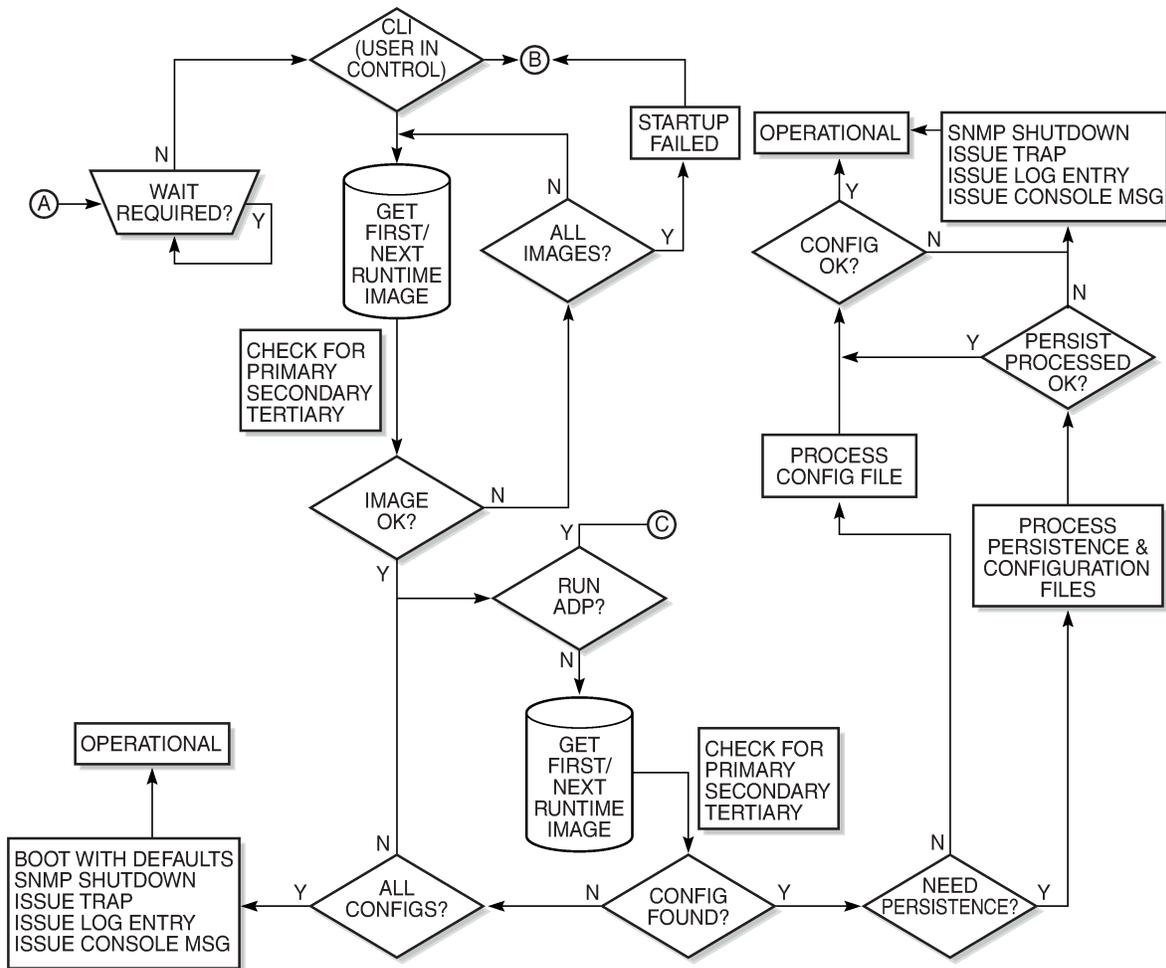
Figure 7: System initialization with ADP shows the boot sequence if Automatic Discovery Protocol (ADP) is run on the system.

Figure 7: System initialization with ADP

SELF-DISCOVERY STAGE

PROVISIONING SUCCESSFUL?

NETWORK DISCOVERY STAGE

EVALUATE/SELECT DHCP OFFER

DHCP SESSION ESTABLISHED?

IP ROUTING ENABLED

CONFIGURATION DISCOVERY STAGE

DISCARD ADP INSTRUCTIONS?

ADP INSTRUCTIONS SUCCESSFUL?

RECOVERABLE ERROR?

ADP FAILED

TEST AND COMMIT STAGE

VALIDATE SYSTEM IP ADDRESS

VALID IP ADDRESS?

PING TEST?

IP ADDRESS PING

PING SUCCESSFUL?

COMMIT CONFIGURATION

APPLY CONFIGURATION UPDATES TO THE BOF FILE

REMOVE ADP KEYWORDS FROM THE BOF FILE

ADP SUCCESSFUL

21815

5.1.3.1 Persistence

The BOF **persist** parameter can specify whether the system should preserve system indexes when a **save** command is executed. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indexes are preserved between reboots, including the interface index, LSP IDs, and path IDs. If persistence is not required and the configuration file is successfully processed, the system becomes operational. If persistence is required, a matching `x.ndx` file must be located and successfully processed before the system can become operational. Matching files (configuration and index files) must have the same filename prefix, such as `test123.cfg` and `test123.ndx`, and are created at the same time when a **save** command is executed. The persistence option must be enabled to deploy the Network Management System (NMS). The default is off.

Traps, logs, and console messages are generated if problems occur, and SNMP shuts down for all SNMP gets and sets; however, traps are issued.

5.1.4 Automatic Discovery Protocol

The Automatic Discovery Protocol (ADP) is triggered by a factory-installed boot option and automates the initial commissioning of 7705 SAR nodes. When the 7705 SAR is started for the first time, an ADP keyword in the BOF causes automatic discovery to run as part of the TiMOS application image. See the appropriate chassis installation guide, "Automatic Discovery Protocol", for more information on ADP.

ADP supports null, dot1q, and qinq encapsulation on:

- all ports on the 6-port Ethernet 10Gbps Adapter card
- all ports on the 8-port Gigabit Ethernet Adapter card
- all ports on the 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)
- all ports on the 6-port SAR-M Ethernet module
- all Ethernet ports on the 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-Wx, and 7705 SAR-X

Caution: For XOR ports, ADP will not run successfully if the connection to the network is made from the SFP connector because the default connector is RJ45.

Note: ADP is not supported on the 4-port SAR-H Fast Ethernet module.

When run on the system, ADP goes through four basic stages:

- Self-discovery
- Network discovery
- Configuration discovery
- Test and commit

5.1.4.1 Self-discovery

During the self-discovery stage, all supported adapter cards and CSMs are detected and automatically provisioned. The 7705 SAR then brings up all Ethernet ports. Depending on the physical connectivity of the port, some ports may fail to come up. If at least one port connected to the transport network becomes operationally up, ADP moves to the next stage.

5.1.4.2 Network discovery

During the network discovery stage, the 7705 SAR sends a DHCP DISCOVER message from all operational ports. Table 16: DHCP DISCOVER message options describes the DHCP DISCOVER message options.

Table 16: DHCP DISCOVER message options

Option	Name	Description
chaddr	Client HW Address	The MAC address of the port

Option	Name	Description
51	Lease Time	Always set to Infinite
60	Class Identifier	The class of 7705 SAR router: ALU-AD | SAR-8 ALU-AD | SAR-18 ALU-AD | SAR-A ALU-AD | SAR-Ax ALU-AD | SAR-H ALU-AD | SAR-Hc ALU-AD | SAR-M ALU-AD | SAR-Wx ALU-AD | SAR-X
61	Client Identifier	Not sent by default, but can be configured to be the chassis MAC address or an operator-defined string
82	Relay Agent Information	Network uplink information, such as circuit ID and gateway address, added by the relay agent, if applicable

No client identifier is sent by default, but you can configure this option during boot-up, or with the **auto-discover** command, to be the chassis MAC address or a unique string. During boot-up, you can also configure the VLAN ID for ADP with dot1q or qinq encapsulation.

The ADP network discovery phase is enhanced to automatically scan the entire VLAN range on every datapath Ethernet port on supported cards and nodes. During startup a new node acts as an ADP client and send DHCP discovery packets across the entire VLAN range to automatically discover the Ethernet virtual connection (EVC) VLAN. If at least one DHCP discovery packet reaches a server and that server responds with a DHCP offer packet, the ADP client node registers the new interface against that server's VLAN.

5.1.4.3 Configuration discovery

During the configuration discovery stage, the DHCP server receives the DHCP DISCOVER message and replies with a DHCP OFFER message that contains an IP address assigned to the network interface. Table 17: DHCP OFFER message options describes the options included in the DHCP OFFER. If any of the required options are not included, the packet may be dropped and not processed.

Table 17: DHCP OFFER message options

Option	Name	Description	Required
yiaddr	Client Ip-Address	The network interface IP address	Yes

Option	Name	Description	Required
		For network consistency, it is recommended that this IP address be a fixed IP address, not assigned randomly from a DHCP server IP pool	
1	Subnet Mask	The network interface subnet mask	Yes
3	Router	The network interface default gateway Only the first router is used – all others are ignored	No
12	Host Name	The network interface hostname	No
51	Lease Time	The least time, validated as infinite	Yes
54	Server Address	Identifies the DHCP server	No
67	Bootfile Name	Contains the ADP instructions or a URL to an ADP instructions file	No

DHCP OFFER messages are not dropped if they contain a yiaddr that does not match the local configured subnets on the DHCP relay interface. This applies only to regular IES and VPRN interfaces with **no lease-populate** configured on the DHCP relay interface.

Option 67 contains further configuration information in the form of keyword text files interpreted by ADP as instructions and executed during the Configuration and Test phases. For basic reachability, option 67 is not mandatory; however, it can be used to send the system IP address of a newly discovered node, making it possible to communicate with the NSP NFM-P and complete ADP.

If a system IP address is made available with the DHCP OFFER and a template configuration file is also executed using the load-cfg keyword, then the system IP address specified in the template configuration file is used instead of the one in the DHCP OFFER.

Table 18: ADP instructions describes the keywords used in ADP instructions. A DHCP offer message can contain a maximum of 15 instructions in either the Bootfile Name option, or in an external file referenced by the include keyword. If more than 15 instructions are included, ADP fails to complete and the system generates an error message in the ADP log.

Table 18: ADP instructions

Keyword	Description	Format
sys-addr	Specifies the system interface IP address and the system base routing instance subnet	sys-addr 10.10.10.1/32
sys-name	Specifies the chassis name	sys-name SITE43_7705
sys-loc	Specifies the chassis location	sys-loc 600_MARCH_ROAD

Keyword	Description	Format
load-cfg	Specifies the URL of a template configuration file to load into the router's runtime configuration	load-cfg ftp://.....@.../7705.cfg
test-ip	Specifies an IP address that must be successfully pinged before committing configuration and declaring ADP a success	test-ip 192.20.2.30
include	Specifies the URL of a file containing additional ADP instructions	include ftp://.....@.../7705.tmp
Any BOF keyword	Interpreted as instructions to update the specified field in the BOF	As per BOF

5.1.4.4 Test and commit

In order for ADP to be declared successful during the test and commit stage, the discovered configuration must contain an IP address. If the optional test-ip keyword is included in the ADP instructions, the node pings the IP address included in the DHCP OFFER message. If ADP is successful, the system stores the configuration and opens an SSH session to provide remote operators access to the router.

ADP can be controlled, without a connected PC or ASCII terminal, by the ACO/LT button on the Fan module. You can use the ACO/LT button to terminate or restart ADP, or reboot the chassis.

Note: The ACO/LT button is not available on the 7705 SAR-A, 7705 SAR-Ax, or 7705 SAR-Wx.

ADP runs in the background to allow continued CLI access for status queries and troubleshooting. Periodic progress updates are sent to the console and can be viewed through a connected PC. Additionally, dump commands are available to display information and detailed logs about ADP during and after running on the system. The logs are not retained over a chassis reboot.

ADP runs only once on a router during initial startup if the automatic discovery is successful. The learned network interface configuration is retained in the local database. On subsequent reboots, the router uses its local database to reload its network configuration. After ADP successfully completes, or if it is manually terminated, the system sends a command to the BOF to remove the ADP keyword. You can terminate ADP at any time while it is running by using the CLI or the ACO/LT button.

Any temporary configuration done by ADP is not stored; however, network configuration and remote access remain enabled to allow the router to be manually provisioned remotely. ADP does not run again on future system reboots unless it is re-enabled via the CLI. If a standby CSM with ADP enabled is inserted into a running system that does not have the ADP keyword in its BOF file, the ADP keyword is automatically removed from the inactive card's BOF file during reconcile.

5.1.5 FIPS-140-2 mode

The 7705 SAR provides the **fips-140-2** boot command to allow a node to run in FIPS-140-2 mode. This mode limits the use of cryptographic algorithms on both the CSM and data plane to only those that are in

accordance with security level 1 of the Federal Information Processing Standards 140 series, version 2 (FIPS-140-2).

FIPS-140-2 mode is supported on the CSM on all 7705 SAR platforms that are equipped with a CSM.

FIPS-140-2 mode is supported on both the CSM and data plane on the following platforms:

- 7705 SAR-8 Shelf V2 and 7705 SAR-18 when equipped with the following adapter cards:
  - 8-port Gigabit Ethernet Adapter card, version 3
  - 2-port 10GigE (Ethernet) Adapter card
  - 10-port 1GigE/1-port 10GigE X-Adapter card, version 2 (supported on the 7705 SAR-18 only)
- 7705 SAR-Ax
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-Wx
- 7705 SAR-X

On the 7705 SAR-A and 7705 SAR-M, FIPS-140-2 mode is supported on the CSM only.

To support the implementation of FIPS-140-2, the TiMOS software image contains an HMAC-SHA-256 secret key that is verified upon boot-up. When FIPS-140-2 is enabled on the node, an HMAC-SHA-256 integrity check is performed during the loading of the both.tim file to ensure that the calculated HMAC-SHA-256 secret key of the loaded image matches that stored in the hmac-sha256.txt file. This is a signature file that has been added to the TiMOS software image and only applies to FIPS-140-2.

> **Note:** The hmac-sha256.txt file must be stored in the same directory as the TiMOS image.

If the image fails the HMAC-SHA-256 check, the node does not boot up, an error message is displayed, and the node tries to reboot the load after a delay of 60 s. The node keeps trying to reboot until the operator cancels the reboot. If the software image is verified by the HMAC-SHA-256 check, the node boots up normally and a message indicating that the software load has passed verification is displayed.

The node performs its normal boot-up sequence, including reading the config.cfg file and loading the configuration. The config.cfg file that is used to boot the node in FIPS-140-2 mode must not contain any configuration that is not supported by the FIPS-140-2 implementation. If such a configuration is present in the config.cfg file when the node boots up, the node loads the config.cfg file until the unsupported configuration is reached and then stops. A failure message is also displayed.

When the node boots in FIPS-140-2 mode, Cryptographic Module Validation Program (CMVP) startup tests are executed on the CSM and applicable data plane. CMVP conditional tests, such as manual key entry tests, pairwise consistency checks, and RNG tests, are executed when required during normal operation.

5.1.5.1 CSM and data path security features and algorithms in FIPS-140-2 mode

Table 19: CSM algorithms and Table 20: Data path algorithms show the CSM and data path security features and associated algorithms for a 7705 SAR node running in FIPS-140-2 mode.

Table 19: CSM algorithms

FIPS-140-2 CSM Algorithms	SSHv2	IPSec (IKEv1, IKEv2)	NGE	SNMPv3	SCP, SFTP	IGP, BGP, MPLS	PKI
Authentication	RSA 2048 DSA 1024 Preference to RSA in SSH negotiation	PSK (DH G14, DH G15)	SSH	N/A	SSH	N/A	N/A
Asymmetric Key	DH G14 (P ≥ 2K prime numbers, q > 224)	DH G14, DH G15 (P ≥ 2K prime numbers, q > 224)	SSH	N/A	SSH	N/A	RSA/ DSA 2048
Symmetric Key	AES-CBC (128, 192, 256) AES-CTR (128, 192, 256) 3DES-CBC	AES-CBC (128, 192, 256) 3DES-CBC	N/A	AES-128	SSH	N/A	N/A
Hash Algorithm	SHA-1 (128) –HMAC-MD5 –HMAC-SHA1-96 –HMAC-MD5-96	SHA-1 (128) SHA-2 (256, 384, 512)	N/A	SHA-1 (SHA-128)	SSH	SHA-1 (128) SHA-2 (256) AES-18-CMAC-96	SHA1 SHA-224 SHA-256 SHA-384 SHA-512
Digital Signature	RSA 2048 DSA 1024	N/A	N/A	N/A	N/A	N/A	RSA/ DSA 2048

Note: MD5 algorithms are not blocked from configuration in FIPS-140-2 mode. Although MD5 is not a FIPS-140-2-approved algorithm, it is allowed to be used when running in FIPS-140-2 mode.

Table 20: Data path algorithms

FIPS-140-2 Data Path Algorithms	SSHv2	IPSec	NGE/L3 Encryption	SNMPv3	SCP, SFTP	IGP, BGP, MPLS
Authentication	N/A	N/A	N/A	N/A	N/A	N/A
Asymmetric Key	N/A	N/A	N/A	N/A	N/A	N/A
Symmetric Key	N/A	AES-CBC (128, 192, 256)	AES-CBC (128, 256)	N/A	N/A	N/A

FIPS-140-2 Data Path Algorithms	SSHv2	IPSec	NGE/L3 Encryption	SNMPv3	SCP, SFTP	IGP, BGP, MPLS
		3DES-CBC				
Hash Algorithm	N/A	SHA-1 (128) SHA-2 (256, 384, 512)	N/A	N/A	N/A	N/A

5.1.5.2 SSHv2 approved algorithms in FIPS-140-2 mode

The following algorithms, configured using the **client-cipher-list** or **server-cipher-list** command, are available for SSHv2 when the node is running in FIPS-140-2 mode:

- aes128-cbc

- aes192-cbc

- aes256-cbc

- aes128-ctr

- aes192-ctr

- aes256-ctr

5.2 Initial system startup process overview

Figure 8: System startup flow displays the process for starting a system that has a removable compact flash. This example assumes that the boot loader, BOF, and the image and configuration files are successfully located. For a system with a non-removable compact flash, the first step in Figure 8: System startup flow does not apply.

Figure 8: System startup flow
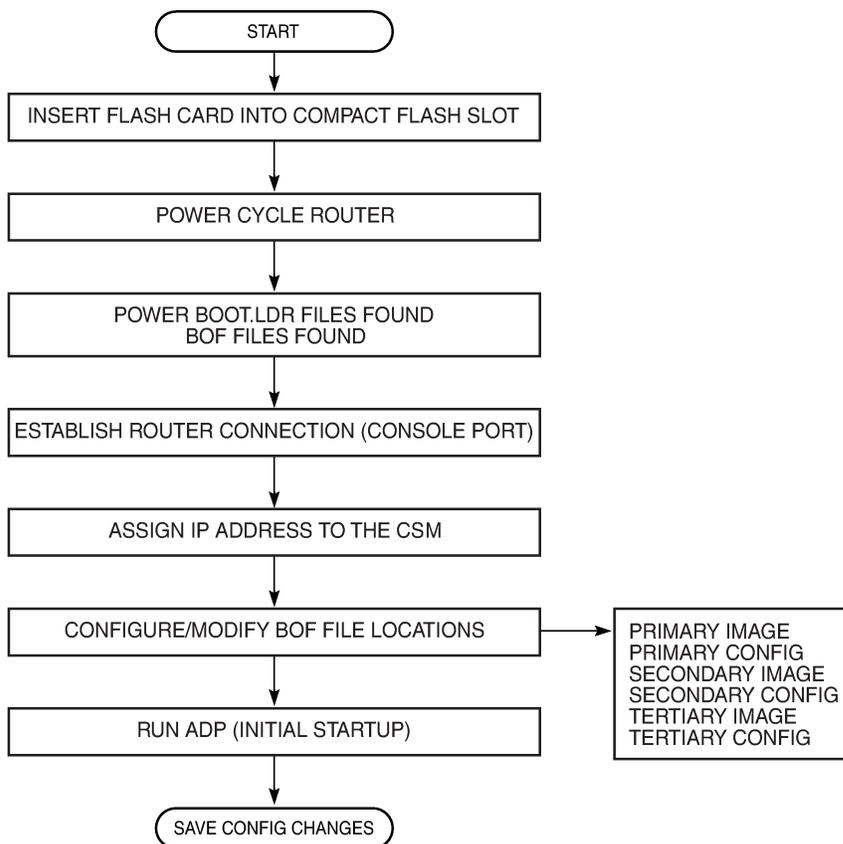
```
                          ┌──────────────┐
                          │    START     │
                          └──────────────┘
                                 │
              ┌──────────────────────────────────────────┐
              │  INSERT FLASH CARD INTO COMPACT FLASH SLOT │
              └──────────────────────────────────────────┘
                                 │
              ┌──────────────────────────────────────────┐
              │          POWER CYCLE ROUTER               │
              └──────────────────────────────────────────┘
                                 │
              ┌──────────────────────────────────────────┐
              │     POWER BOOT.LDR FILES FOUND            │
              │          BOF FILES FOUND                  │
              └──────────────────────────────────────────┘
                                 │
              ┌──────────────────────────────────────────┐
              │  ESTABLISH ROUTER CONNECTION (CONSOLE PORT)│
              └──────────────────────────────────────────┘
                                 │
              ┌──────────────────────────────────────────┐
              │       ASSIGN IP ADDRESS TO THE CSM         │
              └──────────────────────────────────────────┘
                                 │                          ┌──────────────────┐
              ┌──────────────────────────────────────────┐ │ PRIMARY IMAGE    │
              │    CONFIGURE/MODIFY BOF FILE LOCATIONS    │→│ PRIMARY CONFIG   │
              └──────────────────────────────────────────┘ │ SECONDARY IMAGE  │
                                 │                          │ SECONDARY CONFIG │
              ┌──────────────────────────────────────────┐ │ TERTIARY IMAGE   │
              │        RUN ADP (INITIAL STARTUP)          │ │ TERTIARY CONFIG  │
              └──────────────────────────────────────────┘ └──────────────────┘
                                 │
                          ┌──────────────────┐
                          │ SAVE CONFIG CHANGES │
                          └──────────────────┘

                                                          21217
```

5.3 Boot loader file protection

Nokia recommends that the boot loader file on all 7705 SAR platforms be upgraded using a specific command. This command is mandatory on all 7705 SAR platforms that do not have a removable compact flash drive and is part of a mechanism that protects the boot loader file from accidental overwrites on these platforms.

The command checks that the new `boot.ldr` file is a valid image and that it is at least a minimum supported variant for the hardware platform on which it is being loaded. Once this has been verified, the command overwrites the `boot.ldr` file that is stored on the system.

5.3.1 Before upgrading

Before starting the upgrade, all 7705 SAR image files must be copied to the cf3: device on the system. Nokia recommends copying all the image files for a given release into an appropriately named subdirectory off the root directory; for example, cf3:\7705-TiMoS-R6.1.R2. Copying the `boot.ldr` and other files in

a given release to a separate subdirectory ensures that all files for that release are available in case it is necessary to downgrade the software version.

> **Note:** On systems that do not have removable flash drives, you cannot overwrite the `boot.ldr` file in the root directory on cf3:. Instead, copy the file into a subdirectory, or allow the **update boot-loader** command to obtain the file from a network address. Nokia strongly recommends following this process for all 7705 SAR systems.

5.3.2 Performing the upgrade

Upgrade the boot loader file using the command **admin>update boot-loader** *source_url*, where the source URL specifies the new `boot.ldr` filename and its location; for example, in the format cf3:*sub_directory*\boot.ldr.

> **WARNING:** The file upgrade command takes several minutes to complete. Do not reset or power off the system, or insert or remove cards or modules, while the upgrade is in progress, as this could render the system inoperable.

On systems with redundant CSMs, the upgraded boot.ldr file can be copied to the secondary CSM by using the command **admin>redundancy>synchronize boot-env**.

See the latest 7705 SAR Software Release Notes, "Standard software upgrade procedure" section, for complete instructions.

5.4 Accessing the CLI

There are three ways to access management of the 7705 SAR:

- console connection
- Telnet connection
- SSH connection

To access the CLI to configure the software for the first time, follow these steps:

1. Ensure that the CSM is installed and power to the chassis is turned on. The 7705 SAR software then automatically begins the boot sequence.
2. When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

5.4.1 Console connection

To establish a console connection, you need the following:

- an ASCII terminal or a PC running terminal emulation software set to the parameters shown in Table 21: Console configuration parameter values
- a standard serial cable with a male DB9 connector

Table 21: Console configuration parameter values

Parameter	Value
Baud Rate	115 200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Figure 9: 7705 SAR Console port displays an example of the Console port on a 7705 SAR front panel.

Figure 9: 7705 SAR Console port
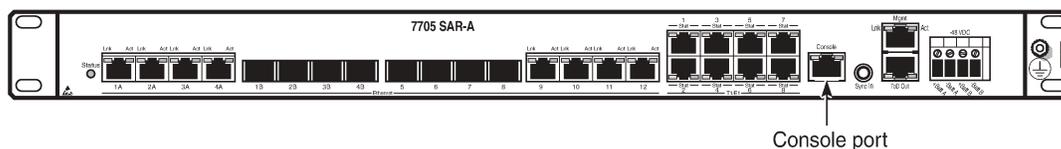
Console port

23319

To establish a console connection:

1. Connect the terminal to the Console port on the front panel (Figure 9: 7705 SAR Console port) using the serial cable.

2. Power on the terminal.

3. Establish the connection by pressing the <Enter> key a few times on your terminal keyboard.

4. At the router prompt, enter the login and password.

The default login is `admin`.

The default password is `admin`.

5.4.2 Telnet connection

Telnet access via a connection to the Management port provides the same options for user and administrator access as those available through the Console port or SSH. You can access the chassis with a Telnet connection from a PC or workstation connected to the network once the following conditions are met:

- the chassis has successfully initialized
- Telnet connections have been enabled using the **config>system>security>telnet-server** (or **telnet6-server**) command
- the Management port has been configured using the **bof>address** command as shown below.

CLI syntax:

```
bof
```

```
    address ip-prefix/ip-prefix-length [active | standby]
```

where:

`address` is an IPv4 (or IPv6) address

5.4.2.1 Running Telnet

After the Management port IP address is configured, the CLI can be accessed with a Telnet connection. To establish a Telnet connection, run a Telnet program and issue the **telnet** command, followed by the Management port IP address.

The following displays an example of a Telnet login:

```
C:\>telnet 192.168.1.xx1
Login: admin
Password: ########
ALU-1#
```

The default login is `admin`.

The default password is `admin`.

5.4.3 SSH connection

SSH access via a connection to the Management port provides the same options for user and administrator access as those available through the console port or Telnet; however, SSH is more secure than Telnet. You can access the chassis with an SSH connection from a PC or workstation connected to the network once the following conditions are met:

- the chassis has successfully initialized

- the Management port has been configured using the **bof>address** command as shown below:

CLI syntax:
```
bof
    address ip-prefix/ip-prefix-length [active | standby]
```

where:

`address` is an IPv4 or IPv6 address

> **Note:** SSH connection attempts after a reboot may generate key warnings as the node generates new SSH keys on each reboot. To avoid these key warnings, enable key preservation using the **config>system>security>ssh>preserve-key** command.

5.4.3.1 Running SSH

After the IP parameters are configured, the CLI can be accessed with an SSH connection. To establish an SSH connection, run an SSH program and issue the SSH command, followed by -l and the username (optional), followed by the IP address.

The following displays an example of an SSH connection with the default admin user (the default password is `admin`).

```
C:\>ssh -l admin 192.168.1.xx1
TiMOS-B-0.0.I2263 both/hops NOKIA SAR 7705
Copyright (c) 2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jul 30 00:11:49 EDT 2016 by csabuild in /rel0.0/I2263/panos/main

admin@192.168.1.xx1's password: ########
```

5.5 Accessing MPT radios connected to a 7705 SAR

The Wavence MPT Craft Terminal Launcher (MCT Launcher) is an application that runs on a Windows PC. By connecting the PC to the 7705 SAR out-of-band Management (Mgmt) port on the active CSM, local MPT radios can be configured and monitored using this application.

To reach both local and remote MPT radios, the PC must be connected to an Ethernet data port on an adapter card and requires a service access point (SAP) to enable in-band management. An IES service together with a local DHCP server configured on the 7705 SAR provides this capability to on-site technicians.

The following output shows a configuration example for a local DHCP server and an IES service.

```
A:SAR18>config>port# info
----------------------------------------------
        description "Craft Port for MW Technicians"
        ethernet
        exit
        no shutdown
----------------------------------------------

*A:SAR18>config>router>dhcp>server# info
----------------------------------------------
                description "DHCP server to serve on-site microwave technician pc"
                pool "craft_pool" create
                    description "Single address pool"
                    use-gi-address
                    subnet 192.168.1.0/30 create
                        options
                            subnet-mask 255.255.255.252
                            default-router 192.168.1.1
                        exit
                        address-range 192.168.1.2 192.168.1.2
                    exit
                exit
                no shutdown
----------------------------------------------

*A:SAR18>config>service>ies>if$ info
----------------------------------------------
                address 192.168.1.1/30
                dhcp
                    server 192.168.1.1
                    gi-address 192.168.1.1
                    no shutdown
                exit
                local-dhcp-server "craft_dhcp_server"
```

```
                sap 1/3/2 create
                exit
---------------------------------------------
```

See the *Wavence MPT Craft Terminal User Manual for Single NE Mode with 7705 SAR* for information about using the MCT Launcher.

5.6 Configuration notes

The following describes BOF configuration guidelines and restrictions.

- For router initialization on devices with a removable compact flash, the compact flash card must be installed in the compact flash slot.

- The loading sequence is based on the order in which it is placed in the configuration file (not based on service ID, for example) and it is loaded as it is read in at boot time.

5.7 Configuring the BOF with the CLI

This section provides information to configure BOF parameters with the CLI.

Topics in this section include:

- BOF configuration overview
- Basic BOF configuration
- Configuring BOF parameters
- Configuring BOF encryption
- Configuration file encryption
- Service management tasks

5.8 BOF configuration overview

The 7705 SAR routers do not contain a boot EEPROM. The boot loader code is loaded from the `boot.ldr` file. The BOF file performs the following tasks:

1. Sets up the CSM Management port (speed, duplex, auto)

2. Assigns the IP address for the CSM Management port

3. Creates static routes for the CSM Management port

4. Sets the console port speed

5. Configures the Domain Name System (DNS) name and DNS servers

6. Configures the primary, secondary, tertiary configuration source

7. Configures the primary, secondary, and tertiary image source

8. Configures operational parameters

Note: The CSM Management port is referred to as the CPM Management port in the CLI to align with the CLI syntax used with other SR products.

5.9 Basic BOF configuration

The parameters that specify the location of the image filename that the router tries to boot from and the configuration file are in the BOF.

The most basic BOF configuration should have the following:

- primary address
- primary image location
- primary configuration location

The following displays an example of a basic BOF configuration.

```
A:ALU-1# show bof
===============================================================================
BOF (Memory)
===============================================================================
    primary-image    ftp://*:*@xxx.xxx.xxx.xx/home/csahwreg17/images/both.tim
    primary-config   ftp://*:*@ xxx.xxx.xxx.xx /home/csahwreg17/images/dut-a.cfg
    address          xxx.xxx.xxx.xx /24 active
    address          xxx.xxx.xxx.xx /24 standby
    primary-dns      xxx.xxx.xxx.xx
    dns-domain       labs.ca.alcatel-lucent.com
    static-route     xxx.xxx.0.0/16 next-hop xxx.xxx.xxx.x
    autonegotiate
    duplex           full
    speed            100
    wait             3
    persist          off
    FIPS-140-2
    console-speed    115200
===============================================================================
A:ALU-1#
```

5.10 Configuring BOF parameters

Use the CLI syntax displayed below to configure BOF parameters:

CLI syntax:
```
bof
    address ip-prefix/ip-prefix-length [active | standby]
    auto-discover
    autonegotiate
    console-speed baud-rate
    dns-domain dns-name
    duplex {full | half}
    encrypt {on | off}
    encryption-key key
    fips-140-2
    password password
```

```
                    persist {on | off}
                    primary-config file-url
                    primary-dns ip-address
                    primary-image file-url
                    save [cflash-id]
                    secondary-config file-url
                    secondary-dns ip-address
                    secondary-image file-url
                    speed speed
                    static-route ip-prefix/ip-prefix-length next-hop ip-address
                    tertiary-config file-url
                    tertiary-dns ip-address
                    tertiary-image file-url
                    wait seconds
```

The following example displays BOF command usage:

Example:

```
ALU-1# bof
ALU-1>bof# address 10.10.10.103/8 active
ALU-1>bof# dns-domain ca.alcatel.com
ALU-1>bof# duplex full
ALU-1>bof# encrypt on
ALU-1>bof# encryption-key hashed
ALU-1>bof# fips-140-2
ALU-1>bof# password hashed
ALU-1>bof# persist on
ALU-1>bof# wait 3
ALU-1>bof# primary-image cf3:\TIMOS.5.0.R0
ALU-1>bof# primary-config cf3:\test123.cfg
ALU-1>bof# primary-dns 10.10.10.103
ALU-1>bof# save cf3:
```

```
A:ALU-1# show bof
===============================================================================
BOF (Memory)
===============================================================================
    primary-image    ftp://*:*@192.168.192.64/cephwreg10/images/both.tim
    primary-config   ftp://*:*@192.168.192.64/cephwreg10/images/dut-a.cfg
    encryption-key   *
    password         *
    address          xxx.xxx.xxx.xx /24 active
    primary-dns      138.120.252.55
    secondary-dns    138.120.252.48
    tertiary-dns     138.120.252.49
    dns-domain       labs.ca.alcatel-lucent.com
    static-route     135.121.0.0/16 next-hop 192.168.192.63
    static-route     138.120.0.0/16 next-hop 192.168.192.63
    static-route     152.148.0.0/16 next-hop 192.168.192.63
    autonegotiate
    duplex           full
    speed            100
    wait             4
    persist          off
    no fips-140-2
    console-speed    115200
    encrypt          on
===============================================================================
A:ALU-1#
```

5.11 Configuring BOF encryption

Use the following CLI syntax to enable encryption of the BOF (bof.cfg) using the AES-256-CBC cipher algorithm.

CLI syntax:

```
bof
    encrypt {on | off}
```

After the BOF is encrypted, it can still be modified using the BOF interactive menu. Access to the BOF interactive menu is controlled using a password.

Use the following syntax to set the interactive menu password.

CLI syntax:

```
bof
    password password [hash | hash2]
```

The password can be in one of the following formats:

- a plaintext string between 8 and 32 characters; the plaintext string cannot contain embedded nulls or end with "hash" or "hash2"

- a hashed string between 1 and 64 characters; the selected hashing scheme can be hash or hash2

Note: The hash2 encryption scheme is node-specific and the password cannot be transferred between nodes.

After the password is set, editing of the BOF during a boot process is allowed only if the password is entered correctly (the boot process can be interrupted in order to make BOF changes). If the password is not entered correctly within 30 s, the node reboots whether the BOF is encrypted or not. This adds an additional layer of security that ensures that the BOF is not exposed to any unauthorized user. After the system is booted, changes can be made to the BOF without entering the password.

Note: After BOF encryption is configured, use the **bof save** command to save the encrypted file.

5.12 Configuration file encryption

Use the following syntax to set the configuration file encryption key using the AES-256-CBC cipher algorithm. This key is used for all configuration files (primary, secondary, and tertiary).

CLI syntax:

```
bof
    encryption-key key [hash | hash2]
```

The encryption key can be in one of the following formats:

- a plaintext string between 8 and 32 characters; the plaintext string cannot contain embedded nulls or end with "hash" or "hash2"

- a hashed string between 1 and 64 characters; the selected hashing scheme can be hash or hash2

> **Note:**
> - The hash2 encryption scheme is node-specific and the key cannot be transferred between nodes.
> - After creating the encryption key, use the **admin save** command to save the encrypted configuration file.
> - If the **admin rollback save** command is used, the rollback files are also encrypted.
> - When an encrypted configuration file is opened in a text editor, editing or viewing the file contents is not possible, as the entire file is encrypted.

5.13 Service management tasks

This section describes system administration commands.

5.13.1 System administration commands

Use the following administrative commands to perform management tasks.

CLI syntax:
```
admin
    display-config
    reboot [active | standby | upgrade] [now]
    save [file-url] [detail] [index]
```

5.13.1.1 Viewing the current configuration

Use the following CLI command to display the current configuration. The **detail** option displays all default values. The **index** option displays only the persistent indexes.

CLI syntax:
```
admin display-config [detail |index]
```

The following displays an example of a configuration file:

```
A:ALU-1# admin display-config
# TiMOS-B-0.0.R3 both/hops NOKIA SAR 7705
# Copyright (c) 2018 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Wed Jan 17 01:05:13 EST 2016 by csabuild in /re8.0/I297/panos/main

# Generated THU JAN 18 21:21:21 2018 UTC

exit all
configure
#------------------------------------------------
echo "System Configuration"
#------------------------------------------------
    system
        name "ALU-1"
exit
        login-control
```

```
            idle-timeout disable
            pre-login-message "CSAxxx - 7705" name
        exit
        time
            sntp
                server-address 192.0.2.37 preferred
                server-address 192.0.2.200
                no shutdown
            exit
            zone EST
        exit
        thresholds
            rmon
            exit
        exit
    exit
#--------------------------------------------------
echo "System Security Configuration"
#--------------------------------------------------
    system
        security
            telnet-server
            ftp-server
            snmp
    exit
...exit all

# Finished THU JAN 17 21:57:11 2016 UTC
A:ALU-1#
```

5.13.1.2 Modifying or deleting BOF parameters

You can modify or delete BOF parameters. The **no** form of these commands removes the parameter from configuration. The changes remain in effect only during the current power cycle unless a **save** command is executed. Changes are lost if the system is powered down or the router is rebooted without saving.

> **Caution:** All BOF parameters can be configured, modified, or deleted locally through a console session or remotely using Telnet or SSH. However, when modifying or deleting the BOF address, the following behaviors must be considered:
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you are running a Telnet IPv6 session or an SSH session, changing or deleting the active IPv4 address will not affect the session.
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you are running a Telnet IPv4 session or an SSH session, changing or deleting the active IPv6 address will not affect the session.
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you change or delete the active IP address that is the same version as the session (for example, you delete the active IPv4 address while running a Telnet IPv4 session), the session will hang once the change executes, and CLI access will be lost. You can either close the session (if possible) or wait until it times out. You must start a new session, using the new or existing active BOF address, to regain CLI access.
>
> - If there is only one active BOF address on the port (that is, not the dual IPv4/IPv6 configuration), and it is deleted through a Telnet or SSH session, the session will hang and CLI access will be lost. You must use a directly connected console session to create a new

BOF address. It is strongly recommended that you do not delete a single active BOF address through Telnet or SSH.

Use the following CLI syntax to remove BOF configuration parameters:

CLI syntax:
```
bof
    save [cflash-id]
```

Example:
```
ALU-1# bof
ALU-1>bof# save cf3:
ALU-1>bof#
bof#
 no address ip-prefix/ip-prefix-length [active | standby]
 no autonegotiate
 no console-speed
 no dns-domain
 encrypt off
 no encryption-key
 no password
 no primary-config
 no primary-dns
 no primary-image
 no secondary-config
 no secondary-dns
 no secondary-image
 no static-route ip-prefix/ip-prefix-length next-hop ip-address
 no tertiary-config
 no tertiary-dns
 no tertiary-image
```

5.13.1.3 Saving a configuration

If you modify a configuration file, the changes remain in effect only during the current power cycle unless a **save** command is executed. Changes are lost if the system is powered down or the router is rebooted without saving.

- Specify the file URL location to save the running configuration. If a destination is not specified, the files are saved to the location where the files were found for that boot sequence. The same configuration can be saved with different filenames to the same location or to different locations.

- The **detail** option adds the default parameters to the saved configuration.

- The **index** option forces a save of the index file.

Use either of the following CLI syntaxes to save a configuration:

CLI syntax:
```
bof
    save [cflash-id]
```

Example:
```
ALU-1# bof
ALU-1>bof# save cf3:
```

```
ALU-1>bof#
```

CLI syntax:

```
admin save [file-url][detail][index]
```

Example:

```
ALU-1# admin save cf3:\test123.cfg
Saving config.# Saved to cf3:\test123.cfg
... complete
ALU-1#
```

> **Note:**
>
> - If the **persist** option is enabled and the **admin save** *file-url* command is executed with an FTP path used as the *file-url* parameter, two FTP sessions simultaneously open to the FTP server. The FTP server must be configured to allow multiple sessions from the same login; otherwise, the configuration and index files will not be saved correctly.
>
> - If BOF encryption is on, the contents of the BOF will be encrypted and unreadable when saved.

5.13.1.4 Saving a configuration to a different filename

Save the current configuration with a unique filename to have additional backup copies and to edit parameters with a text editor. You can save your current configuration to an ASCII file.

Use either of the following CLI syntaxes to save a configuration to a different location:

CLI syntax:

```
bof
    save [cflash-id]
```

Example:

```
ALU-1# bof
ALU-1>bof# save cf3:
ALU-1>bof#
```

or

CLI syntax:

```
admin save [file-url][detail][index]
```

Example:

```
ALU-1>admin save cf3:\testABC.cfg
Saving config.# Saved to cf3:\testABC.cfg
... complete
ALU-1#
```

5.13.1.5 Rebooting

When an **admin>reboot** command is issued, routers with redundant CSMs are rebooted. Changes are lost unless the configuration is saved. Use the **admin>save** *file-url* command to save the current configuration. If no command line options are specified, the user is prompted to confirm the reboot operation.

Use the following CLI syntax to reboot:

CLI syntax:
```
admin
    reboot [active | standby] [now]
```

Example:
```
ALU-1>admin# reboot
A:DutA>admin# reboot

Are you sure you want to reboot (y/n)? y

Resetting...OK

Nokia 7705 Boot ROM. Copyright 2016
Nokia.

All rights reserved. All use is subject to applicable
license agreements.

....
```

5.14 BOF command reference

5.14.1 Command hierarchies

- Configuration commands
- Show commands

5.14.1.1 Configuration commands

```
bof
    - [no] address ip-prefix/ip-prefix-length [active | standby]
    - auto-discover [id client-identifier] [vlan vlan-id]
    - no auto-discover
    - [no] autonegotiate
    - console-speed baud-rate
    - no console-speed
    - dns-domain dns-name
    - no dns-domain
    - duplex {full | half}
    - encrypt {on | off}
    - encryption-key key [hash | hash2]
    - no encryption-key
    - [no] fips-140-2
    - password password [hash | hash2]
    - no password
    - persist {on | off}
    - primary-config file-url
    - no primary-config
    - primary-dns ip-address
    - no primary-dns
    - primary-image file-url
    - no primary-image
    - save [cflash-id]
    - secondary-config file-url
    - no secondary-config
    - secondary-dns ip-address
    - no secondary-dns
    - secondary-image file-url
    - no secondary-image
    - speed speed
    - [no] static-route ip-prefix/prefix-length next-hop ip-address
    - tertiary-config file-url
    - no tertiary-config
    - tertiary-dns ip-address
    - no tertiary-dns
    - tertiary-image file-url
    - no tertiary-image
    - wait seconds
```

5.14.1.2 Show commands

```
show
    - bof [cflash-id | booted]
```

```
            -  boot-messages
```

5.14.2 Command descriptions

- Configuration commands
- Show commands

5.14.2.1 Configuration commands

- File management commands
- BOF processing control commands
- Console port configuration commands
- Image and configuration management commands
- CSM management configuration commands
- DNS configuration commands

5.14.2.1.1 File management commands

bof

Syntax

bof

Context

<root>

Description

This command creates or edits the boot options file (BOF) for the specified local storage device.

A BOF specifies where the system searches for runtime images, configuration files, and other operational parameters during system initialization.

BOF parameters can be modified. Changes can be saved to a specified compact flash. The BOF must be located in the root directory of either an internal or external compact flash local to the system and have the mandatory filename of `bof.cfg`.

When modifications are made to in-memory parameters that are currently in use or operating, the changes are effective immediately. For example, if the IP address of the CSM Management port is changed, the change takes place immediately.

Only one entry of the BOF configuration command statement can be saved after the statement has been found to be syntactically correct.

When opening an existing BOF that is not the BOF used in the most recent boot, a message is issued notifying the user that the parameters do not affect the operation of the node.

The pound (#) sign is used at the beginning of the File syntax. Using the command **file type bof.cfg** displays the # character as a comment delimiter at the top of the raw file. No default BOF exists. The router boots with the factory default boot sequence and options.

Default

n/a

encrypt

Syntax

encrypt {on | off}

Context

bof

Description

This command enables or disables encryption of the BOF (bof.cfg) using the AES256 cipher algorithm.

After the BOF is encrypted, it can still be modified using the BOF interactive menu. Access to the BOF interactive menu is controlled by a password set with the password command.

After BOF encryption is configured, use the **bof save** command to save the encrypted file.

Default

encrypt off

Parameters

on

enables BOF encryption

off

disables BOF encryption

password

Syntax

password *password* [**hash** | **hash2**]

no password

Context

bof

Description

This command configures a password to access the BOF interactive menu at startup.

After the password is configured, the BOF interactive menu is accessible only when the correct password is entered. If the correct password is not entered within 30 s, the node reboots.

The **no** form of this command removes the configured password.

Default
no password

Parameters
password

specifies the password

If the **hash** or **hash2** parameter is not configured, the password is entered in plaintext and the password length must be between 8 and 32 characters. A plaintext password cannot contain embedded nulls or end with "hash" or "hash2".

If the **hash** or **hash2** parameter is configured, the password is hashed and the password length must be between 1 and 64 characters.

hash

specifies that the password is entered in an encrypted form

hash2

specifies that the password is entered in a more complex encrypted form. The **hash2** encryption scheme is node-specific and the password cannot be transferred between nodes.

save

Syntax
save [*cflash-id*]

Context
bof

Description
This command uses the boot option parameters currently in memory and writes them from the BOF to the specified compact flash.

The BOF must be located in the directory of the compact flash drives local to the system and have the mandatory filename of bof.cfg.

The BOF is saved to the compact flash drive associated with the active CSM. The slot name is not case-sensitive. You can use uppercase or lowercase "A" or "B".

Command usage:

- **bof save** — saves the BOF to the default drive (cf3:) associated with the active CSM (either in slot A or B)

- **bof save cf3:** — saves the BOF to cf3: associated with the active CSM (either in slot A or B)

To save the BOF to a compact flash drive associated with the standby CSM (for example, the redundant (standby) CSM is installed in slot B), specify the -A or -B option.

Command usage:

- **bof save cf3-A:** — saves the BOF to cf3: associated with the CSM in slot A whether it is active or standby

- **bof save cf3-B:** — saves the BOF to cf3: associated with the CSM in slot B whether it is active or standby

The slot name is not case-sensitive. You can use uppercase or lowercase "A" or "B".

The **bof save** and **show bof** commands allow you to save to or read from the compact flash of the standby CSM. Use the **show card** command to determine the active and standby CSM (A or B).

Default

saves must be explicitly executed; the BOF is saved to cf3: if a location is not specified

Parameters

cflash-id

the compact flash ID where the **bof.cfg** is to be saved (see Table 14: URL types and syntax for parameter descriptions and values)

5.14.2.1.2 BOF processing control commands

wait

Syntax

wait *seconds*

Context

bof

Description

This command configures a pause, in seconds, at the start of the boot process, which allows system initialization to be interrupted at the console.

When system initialization is interrupted, the operator is allowed to manually override the parameters defined in the BOF.

Only one **wait** command can be defined in the BOF.

Default

3

Parameters

seconds

the time to pause at the start of the boot process, in seconds

Values 1 to 10

5.14.2.1.3 Console port configuration commands

console-speed

Syntax

console-speed *baud-rate*

no console-speed

Context

bof

Description

This command configures the console port baud rate.

When this command is issued while editing the BOF file used for the most recent boot, both the BOF file and the active configuration are changed immediately.

The **no** form of the command reverts to the default value.

Default

115200 — console configured for 115 200 b/s operation

Parameters

baud-rate

the console port baud rate, expressed as a decimal integer

Values 9600, 19200, 38400, 57600, 115200

5.14.2.1.4 Image and configuration management commands

encryption-key

Syntax

encryption-key *key* [**hash** | **hash2**]

no encryption-key

Context

bof

Description

This command creates a key for configuration file encryption and hashing using the AES256 cipher algorithm. This key is used for all configuration files (primary, secondary, and tertiary).

After creating the encryption key, use the **admin save** command to save the encrypted file.

> **Note:** If the **admin rollback save** command is used, the rollback files are also encrypted.

The **no** form of this command deletes the configured encryption key.

Default

no encryption-key

Parameters

key

specifies the encryption key

If the **hash** or **hash2** parameter is not configured, the key is entered in plaintext and the key length must be between 8 and 32 characters. A plaintext key cannot contain embedded nulls or end with "hash" or "hash2".

If the **hash** or **hash2** parameter is configured, the key is hashed and the key length must be between 1 and 64 characters.

hash

specifies that the key is entered in an encrypted form

hash2

specifies that the key is entered in a more complex encrypted form. The **hash2** encryption scheme is node-specific and the key cannot be transferred between nodes.

persist

Syntax

persist {**on** | **off**}

Context

bof

Description

This command specifies whether the system preserves system indexes when a **save** command is executed. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indexes are preserved between reboots, including the interface index, LSP IDs, and path IDs. This reduces resynchronizations of the Network Management System (NMS) with the affected network element.

If **persist** is **on** and the reboot with the appropriate index file fails, SNMP is operationally shut down to prevent the management system from accessing and possibly synchronizing with a partially booted

or incomplete network element. To enable SNMP access, enter the **config>system>snmp>no shutdown**command.

If **persist** is enabled and the **admin save** *<url>* command is executed with an FTP path used as the *<url>* parameter, two FTP sessions simultaneously open to the FTP server. The FTP server must be configured to allow multiple sessions from the same login; otherwise, the configuration and index files are not saved correctly.

> **Note:**
> - Persistency files (.pst) should not be saved on the same disk as the configuration files and the image files.
> - When an operator sets the location for the persistency file, the system checks to ensure that the disk has enough free space. If there is not enough free space, the persistency does not become active and a trap is generated. The operator must free up adequate disk space before persistency becomes active. The system performs a space availability check every 30 seconds. As soon as the space is available the persistency becomes active on the next 30-second check.

Default

off

Parameters

on

preserves the system index when saving the configuration

off

disables the system index saves between reboots

primary-config

Syntax

primary-config *file-url*

no primary-config

Context

bof

Description

This command specifies the name and location of the primary configuration file.

The system attempts to use the configuration specified in **primary-config**. If the specified file cannot be located, the system automatically attempts to obtain the configuration from the location specified in **secondary-config** and then in **tertiary-config**.

If an error in the configuration file is encountered, the boot process aborts.

The **no** form of the command removes the **primary-config** configuration.

Default

n/a

Parameters

file-url

the primary configuration file location (see Table 14: URL types and syntax for parameter descriptions)

primary-image

Syntax

primary-image *file-url*

no primary image

Context

bof

Description

This command specifies the primary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

The **no** form of the command removes the **primary-image** configuration.

Default

n/a

Parameters

file-url

the *location-url* can either be local (this CSM) or a remote FTP server (see Table 14: URL types and syntax for parameter descriptions)

secondary-config

Syntax

secondary-config *file-url*

no secondary-config

Context

bof

Description

This command specifies the name and location of the secondary configuration file.

The system attempts to use the configuration as specified in **secondary-config** if the primary config cannot be located. If the **secondary-config** file cannot be located, the system attempts to obtain the configuration from the location specified in the **tertiary-config**.

If an error in the configuration file is encountered, the boot process aborts.

The **no** form of the command removes the **secondary-config** configuration.

Default

n/a

Parameters

file-url

the secondary configuration file location (see Table 14: URL types and syntax for parameter descriptions)

secondary-image

Syntax

secondary-image *file-url*

no secondary-image

Context

bof

Description

This command specifies the secondary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

The **no** form of the command removes the **secondary-image** configuration.

Default

n/a

Parameters

file-url

the *file-url* can either be local (this CSM) or a remote FTP server (see Table 14: URL types and syntax for parameter descriptions)

tertiary-config

Syntax

tertiary-config file-*url*

no tertiary-config

Context

bof

Description

This command specifies the name and location of the tertiary configuration file.

The system attempts to use the configuration specified in **tertiary-config** if both the primary and secondary config files cannot be located. If this file cannot be located, the system boots with the factory default configuration.

If an error in the configuration file is encountered, the boot process aborts.

The **no** form of the command removes the **tertiary-config** configuration.

Default

n/a

Parameters

file-url

the tertiary configuration file location (see Table 14: URL types and syntax for parameter descriptions)

tertiary-image

Syntax

tertiary-image *file-url*

no tertiary-image

Context

bof

Description

This command specifies the tertiary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

All runtime image files (both.tim) must be located in the same directory.

The **no** form of the command removes the **tertiary-image** configuration.

Default

n/a

Parameters

file-url

the *file-url* can either be local (this CSM) or a remote FTP server (see Table 14: URL types and syntax for parameter descriptions)

5.14.2.1.5 CSM management configuration commands

address

Syntax

[**no**] **address** *ip-prefix/ip-prefix-length* [**active** | **standby**]

Context

bof

Description

This command assigns an IP address to the CSM Management port in the running configuration and the BOF on the active CSM, or the CSM Management port on the standby CSM for systems using redundant CSMs.

Either an IPv4 or IPv6 address can be assigned to the CSM Management port. If an address already exists, it is overwritten with the new address. If no address exists, a new one is created.

Before changing an active IPv4 or IPv6 address, you must ensure that:

• all static routes are removed

• the standby address is removed; address changes are not allowed unless both addresses are on the same subnet

In previous releases, if an IPv6 address was assigned to the CSM Management port, an IPv4 address was also required on the port. This setup is no longer required; therefore, for configurations with both IPv4 and IPv6 addresses, the IPv4 address can be deleted from the BOF.

The **no** form of the command deletes the IP address from the CSM Management port.

If you delete an active IPv4 address from the BOF, or you replace an IPv4 address with an IPv6 address, the following must be considered.

• IPv4 static routes must be removed before the IPv4 active address can be deleted.

• If remote directory locations are used for the primary image file (primary-image) and primary configuration file (primary-config), you must also change the primary image and primary configuration paths (as well as the secondary and tertiary image and configuration files) to use IPv6 addresses. Otherwise, when the 7705 SAR reboots, it tries to load the image using IPv4, which causes continuous reboots.

• If a primary DNS server is configured (primary-dns), the server address must be changed to an IPv6 address in order for it to be reachable.

If the IPv4 address is removed before any Telnet sessions can be established, Telnet IPv6 servers must be enabled using the **config>system>security>telnet6-server** command. See the 7705 SAR System Management Guide for the command description.

> **Caution:**
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you are running a Telnet IPv6 session or an SSH session, changing or deleting the active IPv4 address does not affect the session.
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you are running a Telnet IPv4 session or an SSH session, changing or deleting the active IPv6 address does not affect the session.
>
> - If you have a dual IPv4/IPv6 BOF address configuration and you change or delete the active IP address that is the same version as the session (for example, you delete the active IPv4 address while running a Telnet IPv4 session), the session hangs after the change executes, and CLI access is lost. You can either close the session (if possible) or wait until it times out. You must start a new session, using the new or existing active BOF address, to regain CLI access.
>
> - If there is only one active BOF address on the port (that is, not the dual IPv4/IPv6 configuration), and it is deleted through a Telnet or SSH session, the session hangs and CLI access is lost. You must use a directly connected console session to create a new BOF address. It is strongly recommended that you do not delete a single active BOF address through Telnet or SSH.

Default

no address — there are no IP addresses assigned to CSM Management ports

Parameters

ip-prefix/ip-prefix-length

the IP address for the CSM Management port

active | standby

specifies which CSM Management port address is being configured: the active CSM Management port or the standby CSM Management port

Default   active

auto-discover

Syntax

auto-discover [**id** *client-identifier*][**vlan** *vlan-id*]

no auto-discover

Context

bof

Description

This command enables ADP as part of the boot-up sequence by adding an ADP keyword to the BOF file. ADP runs the next time the chassis is rebooted. You can also use this command to specify an optional unique identifier to use in the automatic discovery broadcast. You can use any unique identifier of up to 16 characters. If you specify mac, the chassis MAC address is used. If you run ADP with 802.1q encapsulation, you can specify the VLAN ID.

Parameters

client-identifier

indicates the unique system identifier to use in the auto-discovery broadcast. If you use MAC as the client identifier, the chassis MAC address is used.

Values   any combination of up to 16 alphanumeric characters with no spaces

vlan-id

indicates the VLAN ID for ADP with 802.1q encapsulation

Values   0 to 4094

autonegotiate

Syntax

[**no**] **autonegotiate**

Context

bof

Description

This command enables speed and duplex autonegotiation on the CSM Management port in the running configuration and the BOF.

When autonegotiation is enabled, the link attempts to automatically negotiate the link speed and duplex parameters. If autonegotiation is enabled, then the configured duplex and speed parameters are ignored.

The **no** form of the command disables the autonegotiate feature on this port.

Default

autonegotiate

duplex

Syntax

duplex {**full** | **half**}

Context

bof

Description

This command configures the duplex mode of the CSM Management port when autonegotiation is disabled in the running configuration and the BOF.

This configuration command allows for the configuration of the duplex mode of the CSM Management port. If the port is configured to autonegotiate, this parameter is ignored.

Default

duplex full — full duplex operation

Parameters

full

> sets the link to full duplex mode

half

> sets the link to half duplex mode

fips-140-2

Syntax

[no]fips-140-2

Context

bof

Description

This command is used to enable the node to support security level 1 of Federal Information Processing Standards 140 series, version 2 (FIPS-140-2). This mode limits the use of cryptographic algorithms on both the CSM and data plane to only those that are in accordance with FIPS-140-2. The node must be rebooted after executing this command in order for the node to begin operating in FIPS-140-2 mode.

> **Caution:** Before using this command, the operator must ensure that no current configuration exists in the configuration file that is not supported in FIPS-140-2 mode. Failing to remove unsupported configurations results in the node being unable to boot up.

The **no** form of the command disables support for security level 1 of FIPS-140-2 on the node.

Default

no fips-140-2

speed

Syntax

speed *speed*

Context

bof

Description

This command configures the speed for the CSM Management port when autonegotiation is disabled in the running configuration and the BOF.

If the port is configured to autonegotiate, this parameter is ignored.

Default

100 — 100 Mb/s operation

Parameters

speed

the link speed, in Mb/s

Values   10, 100, 1000

static-route

Syntax

[**no**] **static-route** *ip-prefix/prefix-length* **next-hop** *ip-address*

Context

bof

Description

This command creates a static route entry for the CSM Management port in the running configuration and the BOF.

This command allows manual configuration of static routing table entries. These static routes are only used by traffic generated by the CSM Management port. To reduce configuration, manual address aggregation should be applied where possible.

A static default route (0.0.0.0/0) cannot be configured on the CSM Management port. A maximum of 10 IPv4 and 10 IPv6 static routes can be configured on the CSM Management port.

Each unique next hop of active static routes configured on both the active and standby CSM Management ports are tested every 60 seconds. If the next hop is unreachable, an alarm is raised. The alarm condition is cleared when the preferred static route becomes reachable.

The **no** form of the command deletes the static route.

Default

n/a

Parameters

ip-prefix/prefix-length

the destination address requiring the static route

next-hop *ip-address*

the next hop IP address used to reach the destination

5.14.2.1.6 DNS configuration commands

dns-domain

Syntax

dns-domain *dns-name*

no dns-domain

Context

bof

Description

This command configures the domain name used when performing DNS address resolution.

This is a required parameter if DNS address resolution is required. Only a single domain name can be configured. If multiple domain statements are configured, the last one encountered is used.

The **no** form of the command removes the domain name from the configuration.

Default

no dns-domain — no DNS domain name is configured

Parameters

dns-name

the DNS domain name

primary-dns

Syntax

primary-dns *ip-address*

no primary-dns

Context

bof

Description

This command configures the primary DNS server used for DNS name resolution.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the primary DNS server from the configuration.

Default

no primary-dns — no primary DNS server is configured

Parameters

ip-address

the IP address of the primary DNS server

secondary-dns

Syntax

secondary-dns *ip-address*

no secondary-dns

Context

bof

Description

This command configures the secondary DNS server for DNS name resolution.

The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the secondary DNS server from the configuration.

Default

no secondary-dns — no secondary DNS server is configured

Parameters

ip-address

the IP address of the secondary DNS server

tertiary-dns

Syntax

tertiary-dns *ip-address*

no tertiary-dns

Context

bof

Description

This command configures the tertiary DNS server for DNS name resolution.

The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the tertiary DNS server from the configuration.

Default

no tertiary-dns — no tertiary DNS server is configured

Parameters

ip-address

the IP address of the tertiary DNS server

5.14.2.2 Show commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

bof

Syntax

bof [*cflash-id* | **booted**]

Context

show

Description

This command displays the BOF executed on the last system boot or on the specified device.

If no device is specified, the BOF used in the last system boot displays. If the BOF has been modified since the system boot, a message displays.

Parameters

cflash-id

the cflash directory name. The slot name is not case-sensitive. Use uppercase or lowercase "A" or "B" for the slot name.

Values   see Table 14: URL types and syntax for parameter descriptions and
values

booted

displays the BOF used to boot the system

Output

The following outputs are examples of BOF information, and Table 22: BOF Field Descriptions describes
the fields.

Output example

```
A:ALU-1# show bof cf3:
===============================================================================
BOF on CF3:
===============================================================================
    primary-image   ftp://*:*@192.168.192.64/cephwreg10/images/both.tim
    primary-config  ftp://*:*@192.168.192.64/cephwreg10/images/dut-a.cfg
    encryption-key  *
    password        *
    address         xxx.xxx.xxx.xx /24 active
    primary-dns     138.120.252.55
    secondary-dns   138.120.252.48
    tertiary-dns    138.120.252.49
    dns-domain      labs.ca.alcatel-lucent.com
    static-route    135.121.0.0/16 next-hop 192.168.192.63
    static-route    138.120.0.0/16 next-hop 192.168.192.63
    static-route    152.148.0.0/16 next-hop 192.168.192.63
    autonegotiate
    duplex          full
    speed           100
    wait            4
    persist         off
    no fips-140-2
    console-speed   115200
    encrypt         on
===============================================================================
A:ALU-1#
```

Output example

```
A:ALU-1# show bof booted
===============================================================================
System booted with BOF
===============================================================================
    primary-image   ftp://*:*@192.168.192.64/cephwreg10/images/both.tim
    primary-config  ftp://*:*@192.168.192.64/cephwreg10/images/dut-a.cfg
    encryption-key  *
    password        *
    address         xxx.xxx.xxx.xx /24 active
    primary-dns     138.120.252.55
    secondary-dns   138.120.252.48
    tertiary-dns    138.120.252.49
    dns-domain      labs.ca.alcatel-lucent.com
    static-route    135.121.0.0/16 next-hop 192.168.192.63
    static-route    138.120.0.0/16 next-hop 192.168.192.63
    static-route    152.148.0.0/16 next-hop 192.168.192.63
    autonegotiate
    duplex          full
    speed           100
```

```
    wait            4
    persist         off
    no fips-140-2
    console-speed   115200
    encrypt         on
================================================================================
A:ALU-1#
```

Table 22: BOF Field Descriptions

Label	Description
primary-image	The primary location of the directory that contains the runtime images of the CSM
primary-config	The primary location of the file that contains the configuration
encryption-key	The encrypted encryption key
password	The encrypted password
address	The IP address and mask associated with the CSM Management port or the secondary CSM Management port
primary-dns	The primary DNS server for resolution of hostnames to IP addresses
secondary-dns	The secondary DNS server for resolution of hostnames to IP addresses
tertiary-dns	The tertiary DNS server for resolution of hostnames to IP addresses
dns-domain	The domain name used when performing DNS address resolution
static-route	The static route entry for the CSM Management port in the running configuration and the BOF
autonegotiate	no autonegotiate — autonegotiate is not enabled
	autonegotiate — autonegotiate is enabled
duplex	half — specifies that the system uses half duplex
	full — specifies that the system uses full duplex
speed	The speed of the CSM Ethernet interface
wait	The time configured for the boot to pause while waiting for console input
persist	Indicates whether the system preserves system indexes when a save command is executed
fips-140-2	Indicates whether FIPS-140-2 is enabled on the node

Label	Description
console speed	The console port baud rate
encrypt	on — BOF encryption is enabled
	off — BOF encryption is not enabled

boot-messages

Syntax

boot-messages

Context

show

Description

This command displays boot messages generated during the last system boot.

Output

The following output is an example of boot messages.

Output example

```
A:ALU-1# show boot-messages
===============================================================================
cf3:/bootlog.txt
===============================================================================
Boot log started on CPU#0
  Build: X-2.1.R1 on Tue Apr 1 16:25:56 EDT 2016 by csabuild

Total Memory: 992MB  Chassis Type: sar8  Card Type: corona_r1
TiMOS-L-2.1.R1 boot/hops NOKIA SAR 7705
Copyright (c) 2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Apr 9 09:36:02 EDT 2016 by csabuild in /rel2.0/b1/R1/panos/main

TiMOS BOOT LOADER
Time from clock is FRI APR 11 13:31:16 2016 UTC
Switching serial output to sync mode...
Total Memory: 992MB  Chassis Type: sar8  Card Type: corona_r1

TiMOS-B-2.1.R1 both/hops NOKIA SAR 7705
Copyright (c) 2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Apr 9 09:53:01 EDT 2016 by csabuild in /rel2.0/b1/R1/panos/main


   ___                   ___            ___            ___
  /\  \                 /\__\          /\  \          /\  \
  \:\  \         ___    /::|  |        /::\  \        /::\  \
   \:\  \       /\__\  /:|:|  |       /:/\:\  \      /:/\ \  \
   /::\  \     _\/__/ /:/|:|__|__    /:/  \:\  \    _\:\~\ \  \
  /:/\:\__\   /\__\  /:/ |::::\__\  /:/__/ \:\__\  /\ \:\ \ \__\
 /:/  \/__/  /:/  /  \/__/~~/:/  /  \:\  \ /:/  /  \:\ \:\ \/__/
```

```
/:/   /     /:/   /           /:/   /   \:\  /:/   /   \:\ \:\__\
\/__/       \/__/           /:/   /    \:\/:/   /    \:\/:/   /
                           /:/   /      \::/   /      \::/   /
                           \/__/         \/__/         \/__/

Time from clock is FRI APR 11 13:31:57 2016 UTC
Initial DNS resolving preference is ipv4-only

CRITICAL: CLI #1001 Cannot locate the configuration file -
Using default configuration values.

MAJOR: CLI #1008 The SNMP daemon is disabled.  To enable SNMP, execute the comma
nd 'config>system>snmp no shutdown'.
TiMOS-B-2.1.R1 both/hops NOKIA SAR 7705
Copyright (c) 2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Apr 9 09:53:01 EDT 2016 by csabuild in /rel2.0/b1/R1/panos/main


Login:
===============================================================================
cf3:/bootlog_prev.txt
===============================================================================
Boot log started on CPU#0
  Build: X-2.1.R1 on Tue Apr 1 16:25:56 EDT 2016 by csabuild

Total Memory: 992MB  Chassis Type: sar8  Card Type: corona_r1
TiMOS-L-2.1.R1 boot/hops NOKIA SAR 7705
Copyright (c) 2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Apr 9 09:36:02 EDT 2016 by csabuild in /rel2.0/b1/R1/panos/main

TiMOS BOOT LOADER
Time from clock is FRI APR 11 13:30:38 2016 UTC
Switching serial output to sync mode...

reboot
===============================================================================
```

6 System management

This chapter provides information about configuring basic system management parameters.

Topics in this chapter include:

- System management parameters
- High availability
- CSM synchronization and redundancy
- Node timing
- System configuration process overview
- Configuration notes
- Configuring system management with CLI
- System command reference

6.1 System management parameters

System management commands allow you to configure basic system management functions such as the system name, the router's location, coordinates, and CLLI code, as well as time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) properties, CRON, and synchronization properties.

6.1.1 System information

System information components include:

- System name
- System contact
- System location
- System coordinates
- Common Language Location Identifier
- System identifier
- PoE power source

6.1.1.1 System name

The system name is the MIB II (RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol* (SNMPv2)) sysName object. By convention, this text string is the node's fully qualified domain name. The system name can be any ASCII printable text string of up to 32 characters.

6.1.1.2 System contact

The system contact is the MIB II sysContact object. By convention, this text string is a textual identification of the contact person for this managed node, together with information about how to contact this person. The system contact can be any ASCII printable text string of up to 80 characters.

6.1.1.3 System location

The system location is the MIB II sysLocation object, which is a text string conventionally used to describe the node's physical location; for example, "Bldg MV-11, 1st Floor, Room 101". The system location can be any ASCII printable text string of up to 80 characters.

6.1.1.4 System coordinates

The Nokia Chassis MIB tmnxChassisCoordinates object defines the system coordinates. This text string indicates the Global Navigation Satellite System (GNSS) coordinates of the location of the chassis.

Two-dimensional GNSS positioning offers latitude and longitude information as a four-dimensional vector:

(direction, hours, minutes, seconds)

where:

direction is one of the four basic values: N, S, W, E

hours range from 0 to 180 (for latitude) and 0 to 90 (for longitude)

minutes and *seconds* range from 0 to 60

<W, 122, 56, 89> is an example of longitude and <N, 85, 66, 43> is an example of latitude.

System coordinates can be expressed in different notations; for example:

- N 45 58 23, W 34 56 12
- N37 37' 00 latitude, W122 22' 00 longitude
- N36 × 39.246' W121 × 40.121

The system coordinates can be any ASCII printable text string up to 80 characters.

6.1.1.5 Common Language Location Identifier

A Common Language Location Identifier (CLLI) code string for the device is an 11-character standardized geographic identifier that uniquely identifies the geographic location of places and specific functional categories of equipment unique to the telecommunications industry. The CLLI code is stored in the Nokia Chassis MIB tmnxChassisCLLICode object.

The CLLI code can be any ASCII printable text string of up to 11 characters.

6.1.1.6 System identifier

A system identifier is a manually configured IPv4 address that can be used to uniquely identify the 7705 SAR in the network in situations where the more commonly used system IP address may change

dynamically, causing loss of historical data attributed to the node. For example, the system IP address can change dynamically using DHCP when the 7705 SAR is acting as a DHCP client and the DHCP server-facing interface is unnumbered. In this situation, a static system identifier may be desirable.

The system identifier can be any IPv4 address.

6.1.1.7 PoE power source

The 7705 SAR-H supports Power over Ethernet (PoE) on all four 10/100/1000 copper Ethernet ports. To use PoE, the PoE power source must be configured at the system level as either internal or external. When the system is configured for the internal PoE power source option, PoE capability can be enabled on ports 5 and 6 only. In addition, port 5 can be enabled for PoE+ but in that case, port 6 cannot support any PoE capability. When the system is configured for the external PoE power source option, a mix of PoE and PoE + is available on ports 5, 6, 7, and 8. See the *7705 SAR-H Chassis Installation Guide*, "Ethernet Ports", for information about supported combinations of PoE and PoE+.

To enable PoE or PoE+ on a PoE-capable port on the 7705 SAR-H, use the **config>port>ethernet>poe** command;see the *7705 SAR Interface Configuration Guide*, "Configuration Command Reference", for more information.

The PoE-capable ports on the 7705 SAR-H act as a Power Source Equipment (PSE) device. They support IEEE 802.3at and IEEE 802.3af.

The 7705 SAR-Wx (variants 3HE07616AA and 3HE07617AA) supports PoE+ on the RJ45 Ethernet port with PoE+. The PoE+ ports are used to deliver power to a "Powered Device", such as a non-line-of-sight (NLOS) or line-of-sight (LOS) microwave radio, at levels compatible with the IEEE 802.3at standard.

To enable PoE+ on a PoE+-capable port on the 7705 SAR-Wx, use the **config>port>ethernet>poe plus** command; see the *7705 SAR Interface Configuration Guide*, "Configuration Command Reference", for more information.

6.1.2 System time

The 7705 SAR routers are equipped with a real-time system clock for time-keeping purposes. When set, the system clock always operates on Coordinated Universal Time (UTC), but the 7705 SAR software has options for local time translation as well as system clock synchronization.

System time parameters include:

- Time zones
- NTP
- SNTP time synchronization
- PTP
- Time-of-day measurement (ToD-1pps)
- GNSS
- CRON

6.1.2.1 Time zones

Setting a time zone in the 7705 SAR allows for times to be displayed in the local time instead of in UTC. The 7705 SAR has both user-defined and system-defined time zones.

A user-defined time zone has a user-assigned name of up to four printable ASCII characters that is different from the system-defined time zones. For user-defined time zones, the offset from UTC is configured as well as any summer time adjustment for the time zone.

The 7705 SAR system-defined time zones are listed in Table 23: System-defined time zones , which includes both time zones with and without summer time correction.

Table 23: System-defined time zones

Acronym	Time zone name	UTC offset
Europe:		
GMT	Greenwich Mean Time	UTC
BST	British Summer Time	UTC +1
IST	Irish Summer Time	UTC +1*
WET	Western Europe Time	UTC
WEST	Western Europe Summer Time	UTC +1
CET	Central Europe Time	UTC +1
CEST	Central Europe Summer Time	UTC +2
EET	Eastern Europe Time	UTC +2
EEST	Eastern Europe Summer Time	UTC +3
MSK	Moscow Time	UTC +3
MSD	Moscow Summer Time	UTC +4
US and Canada:		
AST	Atlantic Standard Time	UTC -4
ADT	Atlantic Daylight Time	UTC -3
EST	Eastern Standard Time	UTC -5
EDT	Eastern Daylight Saving Time	UTC -4
ET	Eastern Time	Either as EST or EDT, depending on place and time of year

Acronym	Time zone name	UTC offset
CST	Central Standard Time	UTC -6
CDT	Central Daylight Saving Time	UTC -5
CT	Central Time	Either as CST or CDT, depending on place and time of year
MST	Mountain Standard Time	UTC -7
MDT	Mountain Daylight Saving Time	UTC -6
MT	Mountain Time	Either as MST or MDT, depending on place and time of year
PST	Pacific Standard Time	UTC -8
PDT	Pacific Daylight Saving Time	UTC -7
PT	Pacific Time	Either as PST or PDT, depending on place and time of year
HST	Hawaiian Standard Time	UTC -10
AKST	Alaska Standard Time	UTC -9
AKDT	Alaska Standard Daylight Saving Time	UTC -8
Australia:		
AWST	Western Standard Time	UTC +8
ACST	Central Standard Time	UTC +9.5
AEST	Eastern Standard/Summer Time	UTC +10

6.1.2.2 NTP

NTP is the Network Time Protocol defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis* and RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*. It allows for the participating network nodes to keep time more accurately and maintain time in a more synchronized fashion among all participating network nodes.

NTP uses stratum levels to define the number of hops from a reference clock. The reference clock is considered to be a Stratum-0 device that is assumed to be accurate with little or no delay. Stratum-0 servers cannot be used in a network. However, they can be directly connected to devices that operate as Stratum-1 servers. A Stratum-1 server is an NTP server with a directly connected device that provides Coordinated Universal Time (UTC), such as a GNSS or atomic clock.

The higher stratum levels are separated from the Stratum-1 server over a network path; therefore a Stratum-2 server receives its time over a network link from a Stratum-1 server. A Stratum-3 server receives its time over a network link from a Stratum-2 server.

The 7705 SAR runs a single NTP clock that operates NTP message exchanges with external NTP clocks. Exchanges can be made with external NTP clients, servers, and peers. These exchanges can be through the base, management, or VPRN routing instances.

When NTP is enabled, the NTP clock in the 7705 SAR operates as an NTP client by default. The 7705 SAR typically operates as a Stratum-2 device, relying on an external Stratum-1 server to source accurate time into the network.

Alternatively, the NTP clock in the 7705 SAR can recover time from a local PTP or GNSS source. This is achieved by configuring the PTP clock or GNSS receiver as the internal system time. The internal system time can then be identified as the preferred source of NTP timing into the network with the command **config>system>time>ntp>server>system-time>prefer**. This configuration makes the local PTP or GNSS source appear as a Stratum-0 server. When the internal PTP clock or GNSS is identified as the server for NTP, NTP promotes the internal NTP server (the 7705 SAR) to Stratum-1 level, which may affect the NTP network topology.

The 7705 SAR can also operate as an NTP server and provide timing to downstream clients with the **ntp-server** command. When the NTP server is enabled with authentication, any NTP clients must authenticate using the correct key.

In server mode, the 7705 SAR advertises the ability to act as a clock source for other network elements. By default, the router transmits NTP packets in NTP version 4 mode. Server mode is supported on the CSM Management port, in the base routing context, and in the VPRN routing context.

As an NTP server, the 7705 SAR can peer with an external NTP server in another router that is considered more trustworthy or accurate than other routers carrying NTP in the system. This allows the peers to act as mutual backups where they can obtain time from or supply time to the other server as required. If both servers are peering each other, the router is in symmetric active mode. This mode requires that the peer association is set on both routers so that the local and remote router designate each other as a peer. If only one server is peering the other (that is, the other peer has not specifically configured the peer association), the router is in symmetric passive mode.

The 7705 SAR can be configured to transmit broadcast NTP packets on a specified interface with the **broadcast** command. The interface can be the management interface, interfaces in the base routing context, or an interface in the VPRN context. The messages are transmitted using a destination address that is the NTP broadcast address. Only IPv4 addressing is supported.

The 7705 SAR can also be configured to receive broadcast NTP packets on interfaces in the base routing context or on the management interface with the **broadcastclient** command.

The router can be configured to transmit or receive multicast NTP packets on the CSM Management port. The **multicast** command configures the transmission of NTP multicast messages. The **multicastclient** command configures the receipt of multicast NTP packets. When receiving or sending multicast NTP messages, the default address 224.0.1.1 is used. Only IPv4 addressing is supported.

The following NTP elements are supported:

- authentication keys — both DES and MD5 authentication are supported as well as multiple keys, to provide increased security support in carrier and other networks

- server and peer addressing — external servers and external peers may be defined using IPv4 or IPv6 addresses

- alert when NTP server is not available — when none of the configured servers are reachable on the node, the system reverts to manual timekeeping and issues a critical alarm. When a server becomes available, a trap is issued indicating that standard operation has resumed.

- NTP and SNTP — if both NTP and SNTP are enabled on the router, SNTP transitions to an operationally down state. If NTP is removed from the configuration or shut down, SNTP resumes an operationally up state.

- NTP priority — if a higher-priority time source such as GNSS or PTP is selected on the router, NTP transitions to an operationally down state. If the higher-priority time source is disqualified or disabled, NTP resumes an operationally up state.

- gradual clock adjustment — because several applications (such as Service Assurance Agent (SAA)) can use the clock, if a major adjustment (128 ms or more) must be performed, the adjustment is performed by programmatically setting the clock. If a minor adjustment (less than 128 ms) must be performed, the adjustment is performed by either speeding up or slowing down the clock.

- to facilitate correct operation when the standby CSM takes over from the active CSM, the time on the secondary CSM must be synchronized with the clock of the active CSM

- to prevent the generation of too many events and traps, the NTP module rate-limits the generation of events and traps to three per second. At that point, a single trap is generated that indicates that event/trap blocking is taking place.

NTP accuracy depends on the accuracy of NTP packet timestamping. By default, NTP packets are timestamped by the CSM where the NTP protocol is executed. However, an enhanced NTP mode is available where the timestamping is performed on the adapter card by the network processor. This reduces variations introduced by packet delay within the router as well as by a busy CPU in the CSM. This enhanced mode is only available for in-band NTP over a network interface. When enhanced NTP mode is used, NTP authentication is not supported.

6.1.2.3 SNTP time synchronization

For synchronizing the system clock with outside time sources, the 7705 SAR includes a Simple Network Time Protocol (SNTP) client. As defined in RFC 2030, SNTP Version 4 is an adaptation of the Network Time Protocol (NTP). SNTP typically provides time accuracy within 100 ms of the time source. SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP is a compact, client-only version of NTP. SNTP does not authenticate traffic.

SNTP can be configured in both unicast client modes (point-to-point) and broadcast client modes (point-to-multipoint). SNTP should be used only at the extremities of the synchronization subnet. SNTP clients should operate only at the highest stratum (leaves) of the subnet and in configurations where no NTP or SNTP client is dependent on another SNTP client for synchronization. SNTP time servers should operate only at the root (Stratum 1) of the subnet and then only in configurations where no other source of synchronization other than a reliable radio clock is available.

The 7705 SAR SNTP client can be configured for either broadcast or unicast client mode.

6.1.2.4 PTP

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard *1588 2008*.

PTP provides the capability to synchronize network elements to a Stratum-1 clock or primary reference clock (PRC) traceable source over a network that may or may not be PTP-aware. PTP has several

advantages over ACR. It is a standards-based protocol, has lower bandwidth requirements, can transport both frequency and time, and can potentially provide better performance.

For more information about PTP, see IEEE 1588v2 PTP.

6.1.2.5 Time-of-day measurement (ToD-1pps)

The 7705 SAR can receive and extract time of day/phase recovery from a 1588 grandmaster clock or boundary clock and transmit the recovered time of day/phase signal to an external device such as a base station through an external time of day port, where available. Transmission is through the ToD or ToD/PPS Out port with a 1 pulse/s output signal. The port interface communicates the exact time of day by the rising edge of the 1 pulse/s signal.

For more information about ToD-1pps, see PTP ordinary timeReceiver clock for time of day/phase recovery.

6.1.2.6 GNSS

The 7705 SAR supports frequency synchronization via a Layer 1 interface such as synchronous Ethernet, and ToD synchronization via a protocol such as NTP or PTP. In cases where these methods are not possible, or where accuracy cannot be ensured for the service, you can deploy a GNSS receiver as a synchronous timing source. GNSS data is used to provide network-independent frequency and ToD synchronization.

GNSS receivers on the following platforms support GPS reference only, or combined GPS and GLONASS reference:

- 7705 SAR-Ax
- 7705 SAR-H with a GPS Receiver module
- 7705 SAR-Wx variants with a GPS RF port
- 7705 SAR-8 Shelf V2 with a GNSS Receiver card
- 7705 SAR-18 with a GNSS Receiver card

A 7705 SAR chassis equipped with a GNSS receiver and an attached GNSS antenna can be configured to receive frequency traceable to Stratum-1 (PRC/PRS). The GNSS receiver provides a synchronization clock to the SSU in the router with the corresponding QL for SSM. This frequency can then be distributed to the rest of the router from the SSU as configured with the **ref-order** and **ql-selection** commands. The GNSS reference is qualified only if the GNSS receiver is operational, has five or more satellites locked, and has a frequency successfully recovered. A PTP timeTransmitter or boundary clock can also use this frequency reference with PTP peers.

In the event of GNSS signal loss or jamming resulting in the unavailability of timing information, the GNSS receiver automatically prevents output of clock or synchronization data to the system, and the system can revert to alternate timing sources.

6.1.2.7 CRON

On the 7705 SAR, the CRON feature supports periodic and date- and time-based scheduling. CRON is used, for example, to schedule Service Assurance Agent (SAA) functions. CRON functions include specifying scripts that need to be run and when they are to be scheduled. Reboots, peer turn-ups,

and SAA tests are scheduled with CRON, as well as OAM events such as connectivity checks or troubleshooting runs.

CRON supports the schedule function. The schedule function is used to configure the type of schedule to run, including one-time-only (one-shot), periodic, or calendar-based runs. All runs are scheduled by month, day, hour, minute, and interval (seconds).

Scripts that have been configured under the **config>system>script-control** context are referenced by the CRON schedule. For information about scripts, see CLI script control.

6.2 High availability

This section discusses the high availability routing options and features available to service providers that help diminish vulnerability at the network or service provider edge and alleviate the effect of a lengthy outage on IP/MPLS networks.

High availability is an important feature in service provider routing and switching systems. High availability is gaining momentum due to the unprecedented growth of IP/MPLS services and applications in service provider networks driven by the demand from the enterprise and residential communities. Downtime can be very costly, and, in addition to lost revenue, customer information and business-critical communications can be lost. High availability is the combination of continuous uptime over long periods (mean time between failures (MTBF)) and the speed at which failover or recovery occurs (mean time to repair (MTTR)).

The popularity of high availability routing is evident at the network or service provider edge where thousands of connections are hosted and rerouting options around a failed piece of equipment can often be limiting. Or, a single access link exists to a customer because of additional costs for redundant links. As service providers converge business-critical services such as real-time voice (VoIP), video, and VPN applications over their IP/MPLS networks, high availability becomes much more stringent compared to the requirements for best-effort data.

Network and service availability become critical aspects when offering advanced IP/MPLS services, which dictate that IP routers that are used to construct the foundations of these networks be resilient to component and software outages.

For high availability configuration information, see CSM synchronization and redundancy.

6.2.1 High availability features

As more and more critical commercial applications move onto the IP/MPLS networks, providing high availability services becomes increasingly important. This section describes high availability features for the 7705 SAR. Most of these features only apply to routers with two Control and Switching Modules (CSMs).

- Redundancy
- Nonstop routing (NSR)
- In-service upgrade
- CSM switchover
- Synchronization

6.2.1.1 Redundancy

The following redundancy features enable the duplication of data elements and software functionality to maintain service continuation in case of outages or component failure.

6.2.1.1.1 Software redundancy

Software outages are challenging even when baseline hardware redundancy is in place. There should be a balance to provide high availability routing; otherwise, router problems typically propagate throughout the service provider network and externally to other connected networks possibly belonging to other service providers. This could affect customers on a broad scale. There are several software availability features that contribute to the percentage of time that a router is available to process and forward traffic.

6.2.1.1.2 Configuration redundancy

Features configured on the active CSM are saved on the standby CSM as well. When the active CSM fails, these features are brought up on the standby CSM that takes over the mastership.

Even with modern modular and stable software, the failure of hardware or software can cause the router to reboot or cause other service impacting events. In the best circumstances, failure leads to the initialization of a redundant route processor, which hosts the standby software configuration to become the active processor.

The 7705 SAR supports hot standby. With hot standby, the router image, configuration, and network state are already loaded on the standby; it receives continual updates from the active route processor and the swap over is immediate. Newer-generation service routers like the 7705 SAR have extra processing built into the system so that router performance is not affected by frequent synchronization, which consumes system resources.

6.2.1.1.3 Component redundancy

7705 SAR component redundancy is critical to reducing MTTR for the routing system. Component redundancy consists of the following features:

- dual Control and Switching modules — for a highly available architecture, redundant Control and Switching Modules (CSMs) are essential
- redundant power supply feed — a power feed can be removed without impact on traffic
- redundant fan — if one fan fails, the others continue to operate and provide cooling to the system without impacting traffic
- hot swap — components in a live system can be replaced or become active without taking the system down or affecting traffic flow to or from other modules

6.2.1.1.4 Service redundancy

During a CSM switchover, dynamically signaled SDPs and services remain up with a minimum loss of forwarded traffic.

6.2.1.1.5 Accounting configuration redundancy

When there is a switchover and the standby CSM becomes active, the accounting servers are checked, and if they are administratively up and capable of coming online (media present and so on), then the standby is brought online and new accounting files are created at that point. Users must manually copy the accounting records from the failed CSM.

6.2.1.1.6 Multi-chassis LAG redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

> **Note:** The 7705 SAR nodes must be of the same type, except for the 7705 SAR-8 Shelf V2 and 7705 SAR-18, which can be used together in a redundant-pair configuration.

A peer is configured by specifying its IP address, to which the MCCP packets are sent. The LAG ID, system priority, and MAC address for the MC-LAG are also configured under the peer. Up to 16 MC-LAGs can be configured and they can either use the same peer or different peers up to a maximum of 4 peers.

It is possible to specify the remote LAG ID in the MC-LAG lag command to allow the local and remote LAG IDs to be different on the peers. If there are two existing nodes which already have LAG IDs that do not match, and an MC-LAG is created using these nodes, then the remote LAG ID must be specified so that the matching MC-LAG group can be found. If no matching MC-LAG group is found between neighbor systems, the individual LAGs operates and no MC-LAG operation is established.

Two timer options, **keep-alive-interval** and **hold-on-neighbor-failure**, are available in the MC-LAG configuration. The **keep-alive-interval** option specifies the frequency of the messages expected to be received from the remote peer and is used to determine if the remote peer is still active. If **hold-on-neighbor-failure** messages are missed, then it is assumed that the remote peer is down.

Figure 10: MC-LAG at Access and Aggregation Sites shows an example of MC-LAG deployed at access and aggregation sites.

Figure 10: MC-LAG at Access and Aggregation Sites
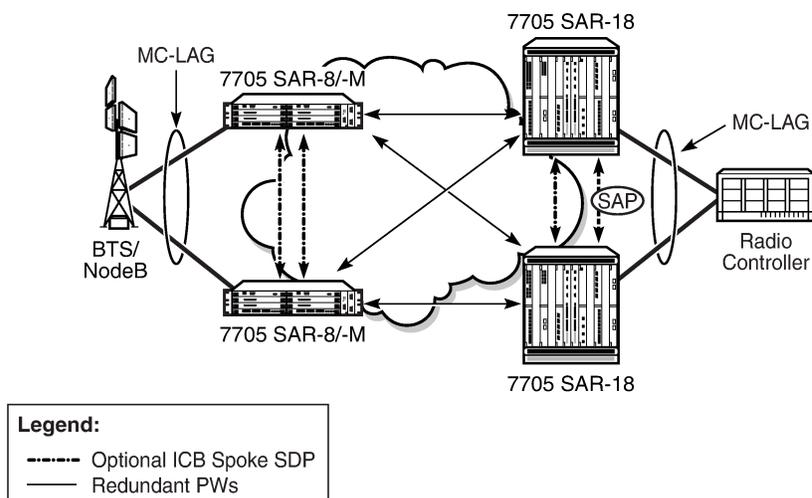
Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

> **Note:** A 7705 SAR node in an MC-LAG configuration that has an ICB spoke SDP configured on it with the MC-LAG in standby mode does not terminate Ethernet CFM frames. It transparently switches the frames to the other node of the MC-LAG group. This mode of operation is consistent with the 7705 SAR operating in S-PE mode.

Enabling the LAG **slave-to-partner** parameter ensures synchronized activity switching between the multi-chassis and the single-chassis endpoints. When multi-chassis endpoints are configured in slave-to-partner mode, multi-chassis endpoints always follow the single-chassis activity. The link that is promoted as active via the single-chassis endpoint is used as the active link. Enabling **slave-to-partner** ensures that out-of-sync scenarios do not occur for the LAG. A multi-chassis pair with pseudowire redundancy and ICBs is always able to direct traffic to the active endpoint, so enabling **slave-to-partner** does not impose any risk on the network side.

MC-LAG includes support for hash–based peer authentication, configurable heartbeat timers between peers, heartbeat multiplier, LAG bound to MC-LAG with LACP and support for any valid IP link between peers for the multi-chassis Control Protocol (MCCP). MC-LAG supports a configurable fault propagation delay and also provides an option to shut down a MEP on a standby endpoint.

MC-LAG maintains state across a CSM switchover event. The switchover event is transparent to peer MC-LAG nodes where sessions and state are preserved. MC-LAG is supported on the following platforms, adapter cards, and modules:

• 8-port Gigabit Ethernet Adapter card

- 6-port Ethernet 10Gbps Adapter card
- 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)
- Packet Microwave Adapter card
- 6-port SAR-M Ethernet module
- 7705 SAR-M (the port must be in access mode and autonegotiation must be off or limited)
- 7705 SAR-X

Note: The 7705 SAR only supports MC-LAG for Epipes and VPLS.

6.2.1.2 Nonstop routing (NSR)

With NSR on the 7705 SAR, routing neighbors are unaware of a routing process fault. If a fault occurs, a reliable and deterministic activity switch to the inactive control complex occurs such that routing topology and reachability are not affected, even in the presence of routing updates. NSR achieves high availability through parallelization by maintaining up-to-date routing state information, at all times, on the standby route processor. This capability is achieved independently of protocols or protocol extensions, providing a more robust solution than graceful restart protocols between network routers.

The NSR implementation on the 7705 SAR applies to all supported routing protocols. NSR makes it possible to keep the existing sessions (such as LDP) during a CSM switchover, including support for MPLS signaling protocols. Peers do not see any change.

Traditionally, high availability issues have been patched through non-stop forwarding solutions. NSR overcomes these limitations by delivering an intelligent hitless failover solution.

The following NSR entities remain intact after a switchover:

- ATM/IMA VPs/VCs
- LDP
- PPP and MLPPP sessions
- RIP neighbors

6.2.1.3 In-service upgrade

In-service upgrades allow new routing engine software and microcode to be installed on the 7705 SAR while existing services continue to operate. Software upgrades can be performed only for specific maintenance releases (generally R4 loads and higher). Software upgrades also require NSR. If software or microcode on the CSM needs to be upgraded, CSM redundancy is required.

Note: The in-service upgrade requires the adapter cards to be reset. This causes a short outage.

Follow the steps below to upgrade routing engine software on the 7705 SAR without affecting existing services:

1. Install new software on the standby CSM.
2. Reboot the standby CSM for the new software to take effect.

3. Perform a manual switchover on the active CSM by using the force-switchover command on the CLI. The standby CSM becomes the active CSM, placing the formerly active CSM into standby.

4. Repeat steps 1 and 2 to upgrade the standby CSM.

6.2.1.4 CSM switchover

During a switchover, system control and routing protocol execution are transferred from the active to the standby CSM. A switchover may occur automatically or manually.

An automatic switchover may occur under the following conditions:

- a fault condition arises that causes the active CSM to crash or reboot

- the active CSM is declared down (not responding)

- online removal of the active CSM

Users can manually force the switchover from the active CSM to the standby CSM by using the **admin redundancy force-switchover now** CLI command or the **admin reboot active** [**now**] CLI command.

With the 7705 SAR, the **admin reboot active** [**now**] CLI command does not cause both CSMs to reboot.

6.2.1.5 Synchronization

Synchronization between the CSMs includes the following:

- Configuration and boot-env synchronization
- State database synchronization

6.2.1.5.1 Configuration and boot-env synchronization

Configuration and boot-env synchronization are supported in **admin>redundancy> synchronize** and **config>redundancy>synchronize** contexts.

6.2.1.5.2 State database synchronization

If a new standby CSM is inserted into the system, it synchronizes with the active CSM upon a successful boot process.

If the standby CSM is rebooted, it synchronizes with the active CSM upon a successful boot process.

When configuration or state changes occur, an incremental synchronization is conducted from the active CSM to the standby CSM.

If the synchronization fails, the standby CSM does not reboot automatically. The **show redundancy synchronization** command displays synchronization output information.

If the active and standby CSMs are not synchronized for some reason, users can manually synchronize the standby CSM by rebooting the standby by issuing the **admin reboot standby** command.

6.3 CSM synchronization and redundancy

The 7705 SAR uses a 1:1 redundancy scheme. Redundancy methods facilitate system synchronization between the active and standby CSMs so that they maintain identical operational parameters to prevent inconsistencies in the event of a CSM failure.

When automatic system synchronization is enabled for an entity, any save or delete file operations configured on the primary, secondary, or tertiary choices on the active CSM file system are mirrored in the standby CSM file system.

Although software configurations and images can be copied or downloaded from remote locations, synchronization can only occur locally between compact flash drives (cf3-A: and cf3-B:).

Synchronization can occur:

- automatically — automatic synchronization is disabled by default. To enable automatic synchronization, the **config>redundancy>synchronize** command must be specified with either the **boot-env** parameter or the **config** parameter.

  When the **boot-env** parameter is specified, the BOF, boot.ldr, config, and image files are automatically synchronized. When the **config** parameter is specified, only the config files are automatically synchronized.

  Automatic synchronization also occurs whenever the BOF is modified with persistence on and when an **admin>save** command is entered with no filename specified.

- manually — to execute synchronization manually, the **admin>redundancy> synchronize** command must be entered with the **boot-env** parameter or the **config** parameter.

  When the **boot-env** parameter is specified, the BOF, boot.ldr, config, and image files are synchronized. When the **config** parameter is specified, only the config files are synchronized.

The following shows the output displayed during a manual synchronization of configuration files.

```
ALU-1>admin>redundancy# synchronize config

Syncing configuration......

Syncing configuration.....Completed.
ALU-1#
```

6.3.1 Active and standby designations

Typically, the first CSM installed in a 7705 SAR chassis assumes the role as active, regardless of being inserted in Slot A or B. The next CSM installed in the same chassis then assumes the role as the standby CSM. If two CSMs are inserted simultaneously (or almost simultaneously) and are booting at the same time, preference is given to the CSM installed in Slot A.

If only one CSM is installed in a 7705 SAR, it becomes the active CSM regardless of the slot it is installed in.

To visually determine the active and standby designations, the MS/CTL LED on the faceplate is lit green (steady) to indicate the active designation. The MS/CTL LED on the second CSM faceplate is flashing green to indicate the standby designation.

The following output shows that the CSMv2 installed in Slot A on a 7705 SAR-8 Shelf V2 is acting as the active CSM and the CSMv2 installed in Slot B is acting as the standby.

```
ALU-1# show card
===============================================================================
Card Summary
===============================================================================
Slot   Provisioned Type                        Admin Operational   Comments
          Equipped Type (if different)         State State
-------------------------------------------------------------------------------
1      iom-sar                                 up    up
A      csmv2-10g                               up    up/active
B      csmv2-10g                               up    down/standby
===============================================================================
```

6.3.2 When the active CSM goes offline

When an active CSM goes offline (because of reboot, removal, or failure), the standby CSM takes control without rebooting or initializing itself. It is assumed that the CSMs are synchronized; therefore, there is no delay in operability. When the CSM that went offline boots and then comes back online, it becomes the standby CSM.

6.3.3 Persistence

The persistence feature allows lease information about DHCP servers to be kept across reboots. This information can include data such as the IP address, MAC binding information, and lease length information.

The system performs the following tasks to make data persistent. In systems with only one CSM, only task 1 applies. In systems with dual CSMs, both tasks apply.

1. When a DHCP ACK is received from a DHCP server, the entry information is written to the active CSM compact flash. If persistence fails completely (bad cflash), a trap is generated indicating that persistence can no longer be guaranteed.

2. DHCP message information is sent to the standby CSM, and the DHCP information is also written to the compact flash. If persistence fails on the standby CSM also, a trap is generated.

6.3.4 Administrative tasks

This section contains information to perform administrative tasks:

• Saving configurations

• Specifying post-boot configuration files

6.3.4.1 Saving configurations

Whenever configuration changes are made, the modified configuration must be saved so that it is not lost when the system is rebooted.

Configuration files are saved by executing explicit command syntax that includes the file URL location to save the configuration file as well as options to save both default and non-default configuration parameters. Boot options file (BOF) parameters specify where the system should search for configuration and image files as well as other operational parameters during system initialization.

For more information about the BOF, see the chapter on Boot options in this guide.

6.3.4.2 Specifying post-boot configuration files

Two post-boot configuration extension files are supported and are triggered when either a successful or failed boot configuration file is processed. The **boot-bad-exec** and **boot-good-exec** commands specify URLs for the CLI scripts to be run following the completion of the boot-up configuration. A URL must be specified or no action is taken.

For example, after a configuration file is successfully loaded, the specified URL can contain a nearly identical configuration file with specific commands enabled or disabled, or particular parameters specified and according to the script which loads that file.

6.3.5 Automatic synchronization

Use the CLI syntax displayed below to configure synchronization components relating to active-to-standby CSM switchover. In redundant systems, synchronization ensures that the active and standby CSMs have identical operational parameters, including the active configuration, CSM, and IOM images in the event of a failure or reset of the active CSM.

The **force-switchover** command forces a switchover to the standby CSM card.

To enable automatic synchronization, either the **boot-env** parameter or the **config** parameter must be specified. The synchronization occurs when the **admin save** or **bof save** commands are executed.

When the **boot-env** parameter of the **synchronize** command is specified, the BOF, boot.ldr, config, and image files are automatically synchronized. When the **config** parameter is specified, only the configuration files are automatically synchronized.

Synchronization also occurs whenever the BOF is modified with persistence on and when an **admin>save** command is entered with no filename specified.

6.3.5.1 Boot-env option

The **boot-env** option enables a synchronization of all the files used in system initialization.

When configuring the system to perform this synchronization, the following occurs:

1. The BOF used during system initialization is copied to the same compact flash on the standby CSM (in redundant systems).

   Note: The synchronization parameters on the standby CSM are preserved.

2. The primary, secondary, and tertiary images (provided they are locally stored on the active CSM) are copied to the same compact flash on the standby CSM.

3. The primary, secondary, and tertiary configuration files (provided they are locally stored on the active CSM) are copied to the same compact flash on the standby CSM.

6.3.5.2 Config option

The **config** option synchronizes configuration files by copying the files specified in the active CSM BOF file to the same compact flash on the standby CSM.

6.3.6 Manual synchronization

The **admin redundancy synchronize** command performs manual CSM synchronizations. The **boot-env** parameter synchronizes the BOF, image, and configuration files in redundant systems. The **config** parameter synchronizes only the configuration files in redundant systems.

6.3.6.1 Forcing a switchover

The **force-switchover now** command forces an immediate switchover to the standby CSM card.

If the active and standby CSMs are not synchronized for some reason, users can manually synchronize the standby CSM by rebooting the standby by issuing the **admin reboot standby** command on the active CSM.

6.4 Node timing

The 7705 SAR supports a centralized synchronization system with an SSU in each CSM. The SSU can be synchronized to a traceable primary reference clock through an external timing port, line interface, or timing-over-packet technology. The transmit clock of each T1/E1, DS3/E3, SONET/SDH port or synchronous Ethernet-capable port (referred to as a synchronous Ethernet port in this guide) can then be configured to use the node clock or alternatives.

The 7705 SAR supports three timing references — one external and two internal. The timing references can be configured as an ordered list of highest to lowest priority. The system uses an available valid timing reference with the highest priority. If a failure on the current timing reference occurs, the next highest timing reference takes over. The reference switching can be configured to operate in a revertive or non-revertive manner with the **sync-if-timing revert** command. Revertive switching always selects the highest-priority valid timing reference as the current source. If a reference with a higher priority becomes valid, the system automatically switches to that timing reference. Non-revertive switching means that the active timing reference remains selected while it is valid, even if a higher-priority timing reference becomes available. If the current timing reference becomes invalid, then a switch to the highest-priority available timing reference is initiated. If all the timing references fail or have not been configured, the SSU enters holdover mode of its Stratum 3 oscillator (if it was previously synchronized) or free-run mode.

The external timing reference input with a 2.048 MHz G.703 signal, 5 MHz sine wave, or 10 MHz sine wave, is available directly on the following:

- 7705 SAR-M
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-A
- 7705 SAR-Ax

- 7705 SAR-X

The CSMv2 on the 7705 SAR-8 Shelf V2 does not support a 5 MHz signal. On the 7705 SAR-18, the external timing reference input with a 2.048 MHz G.703, T1 (100 Ω), or E1 (120 Ω), is supported by the BITS ports 1 and 2 located on the Alarm module.

The two internal timing references originate from timing extracted from interface ports. This timing can be recovered directly from physical layer framing on a T1/E1 port, from adaptive timing recovery for TDM pseudowires, or from a synchronous Ethernet port.

On the 7705 SAR-M, all RJ45 Ethernet ports and SFP ports support synchronous Ethernet and can supply a timing reference to be used as a source of node synchronization. On the 7705 SAR-M variants with T1/E1 ports, two T1/E1 ports can supply a timing reference. The 2-port 10GigE (Ethernet) module or 6-port SAR-M Ethernet module can supply two timing references.

On the 7705 SAR-H and 7705 SAR-Hc, all RJ45 Ethernet ports and SFP ports support synchronous Ethernet and can supply a timing reference to be used as a source of node synchronization. When the 4-port T1/E1 and RS-232 Combination module is installed in the 7705 SAR-H, a single T1/E1 port on the module can supply a timing reference; it can be independently configured for loop-timing or node-timing. When the GPS Receiver module is installed in the 7705 SAR-H, the GPS RF port can be used as a source of node synchronization.

On the 7705 SAR-A, all synchronous Ethernet ports can supply a timing reference to be used as a source of node synchronization. Synchronous Ethernet is supported on the XOR ports (1 to 4), configured as either RJ45 ports or SFP ports. Synchronous Ethernet is also supported on SFP ports 5 to 8. Ports 9 to 12 do not support synchronous Ethernet (except when 10/100/1000BaseT copper SFP is used) and, therefore, cannot be used as a timing reference. On the 7705 SAR-A variant with T1/E1 ports, two T1/E1 ports can also supply a timing reference.

On the 7705 SAR-Ax, all Ethernet ports support synchronous Ethernet and IEEE 1588v2 PTP and can supply a timing reference to be used as a source of node synchronization. The 7705 SAR-Ax can also derive its timing from a GPS antenna signal using the GNSS RF port.

On the 7705 SAR-Wx, all RJ45 Ethernet ports and SFP ports support synchronous Ethernet and IEEE 1588v2 PTP, and can supply a timing reference to be used as a source of node synchronization. For 7705 SAR-Wx variants with a GPS RF port, the GPS RF port can be used as a source of node synchronization.

On the 7705 SAR-X, all Ethernet ports support synchronous Ethernet and IEEE 1588v2 PTP. Ethernet ports and T1/E1 ports can supply two timing references to be used as a source of node synchronization. In addition, each T1/E1 port can be independently configured for loop timing.

The 7705 SAR-8 Shelf V2 and 7705 SAR-18 can receive one or two timing references depending on the port and card type supplying the reference. A timing reference can come from:

- a single SONET/SDH port on the 4-port OC3/STM1 Clear Channel Adapter card

- two DS3/E3 ports on the 4-port DS3/E3 Adapter card

- two SONET/SDH ports on the 2-port OC3/STM1 Channelized Adapter card or 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card

- two synchronous Ethernet ports on:

  - the 6-port Ethernet 10Gbps Adapter card

  - the 8-port Gigabit Ethernet Adapter card

  - the 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)

  - the 2-port 10GigE (Ethernet) Adapter card

- two T1/E1 ports on the 16-port T1/E1 ASAP Adapter card or the 32-port T1/E1 ASAP Adapter card. References must be from different framers; the framers each have eight ports and are grouped as ports 1 to 8, 9 to 16, 17 to 24, and 25 to 32.

- two ports on the Packet Microwave Adapter card: on port 1 or 2, it could be a synchronous Ethernet or PCR-enabled port; on port 3 or 4, it could be a synchronous Ethernet (optical SFP only) or PCR-enabled port (copper-based SFP only); on ports 5 through 8, it could be a synchronous Ethernet (optical SFP only) port.

- the GNSS RF port on the GNSS Receiver card

The 7705 SAR-8 Shelf V2 and 7705 SAR-18 can also use IEEE 1588v2 PTP as a source of node synchronization.

Each T1/E1 port can be independently configured for loop-timing (recovered from an Rx line) or node-timing (recovered from the SSU in the active CSM).

In addition, T1/E1 CES circuits on the following can be independently configured for adaptive timing (clocking is derived from incoming TDM pseudowire packets):

- 16-port T1/E1 ASAP Adapter card

- 32-port T1/E1 ASAP Adapter card

- 7705 SAR-M (variants with T1/E1 ports)

- 7705 SAR-A (variant with T1/E1 ports)

- T1/E1 ports on the 4-port T1/E1 and RS-232 Combination module

T1/E1 CES circuits on the following can be independently configured for differential timing (recovered from RTP in TDM pseudowire packets):

- 16-port T1/E1 ASAP Adapter card

- 32-port T1/E1 ASAP Adapter card

- 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card (DS1/E1 channels)

- 4-port DS3/E3 Adapter card (DS1/E1 channels on DS3 ports; E3 ports cannot be channelized); DCR on DS1/E1 channels is supported only on the first three ports of the card

- 7705 SAR-M (variants with T1/E1 ports)

- 7705 SAR-A (variant with T1/E1 ports)

- T1/E1 ports on the 4-port T1/E1 and RS-232 Combination module

Adaptive timing and differential timing are not supported on DS1 or E1 channels that have CAS signaling enabled.

A T1/E1 port can be configured to be a timing source for the node.

Each SONET/SDH port and each T1/E1 CES circuit on a 2-port OC3/STM1 Channelized Adapter card can be independently configured to be loop-timed or node-timed; each DS3 circuit can be independently configured to be loop-timed or free-run. A SONET/SDH port can be configured to be a timing source for the node.

Each SONET/SDH port on a 4-port OC3/STM1 Clear Channel Adapter card can be independently configured to be loop-timed or node-timed. A SONET/SDH port can be configured to be a timing source for the node.

Each SONET/SDH port on a 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card can be independently configured to be node-timed; each T1/E1 CES circuit can be independently configured to be node-timed, loop-timed, or differential-timed. A SONET/SDH port can be configured to be a timing source for the node.

Each clear channel DS3/E3 port on a 4-port DS3/E3 Adapter card can be independently configured to be loop-timed, node-timed, or differential-timed. When a DS3 port is channelized, each DS1 or E1 channel can be independently configured to be loop-timed, node-timed, or differential-timed (differential timing on DS1/E1 channels is supported only on the first three ports of the card). When not configured for differential timing, a DS3/E3 port can be configured to be a timing source for the node.

6.4.1 External timing mode

The external input and output timing ports are located on the CSM on the 7705 SAR-8 Shelf V2 and directly on the 7705 SAR-H and 7705 SAR-M. The 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-X have an external timing input port only, located on their faceplates. The external input timing port allows the SSU to be synchronized to an external timing reference. The external output timing port provides a synchronization output signal from the 7705 SAR to an external device. These external timing references typically would come from a GNSS, Building Integrated Timing System (BITS), or the external output timing ports from other telecom equipment.

The timing ports can be configured for the following:

- 2.048 MHz G.703 section 13 signal
- 5 MHz sine wave (not available on the 7705 SAR-8 Shelf V2 CSMv2)
- 10 MHz sine wave

On the 7705 SAR-18, the BITS ports 1 and 2 can be configured for the following:

- 2.048 MHz G.703 section 13 signal
- T1 (ESF or SF)
- E1 (PCM30CRC or PCM31CRC)

When redundant CSMs are used on the 7705 SAR-8 Shelf V2, the external synchronization inputs in each CSM must come from the same synchronization source; that is, you cannot select each input of the two CSMs as two of the three timing references. A Y-cable can be used to connect to a single reference connector. The synchronization output on each CSM is clocked by its own SSU clock.

On the 7705 SAR-18, either BITS port 1 or port 2 is available as an input and output source. When both inputs are connected and available, then the quality level (QL) from Synchronization Status Messaging (SSM) is used to determine which port is used by the CSMs as the BITS input. If SSM is not available, then BITS port 1 is the preferred input. BITS port 2 is used if BITS port 1 is not available. In this case, the operation is non-revertive. The BITS output ports 1 and 2 are clocked by the active CSM's SSU clock.

The BITS output **source** command can be used to configure the BITS output ports' source path on the 7705 SAR-18 to be either:

- the filtered clock from the Synchronous Equipment Timing Generator (SETG)
- the alternate unfiltered path from the BITS output port via Selector A and C, as per ITU-T G.8262

Figure 11: BITS timing source path shows an example of a timing source path. The BITS port is configured to deliver an input reference directly to a dedicated timing device such as a BITS or standalone synchronization equipment (SASE) device in a customer facility. The external BITS clock can have multiple references and can provide a common high-quality clock to all network elements at the customer location, including the 7705 SAR-18 node.

Figure 11: BITS timing source path
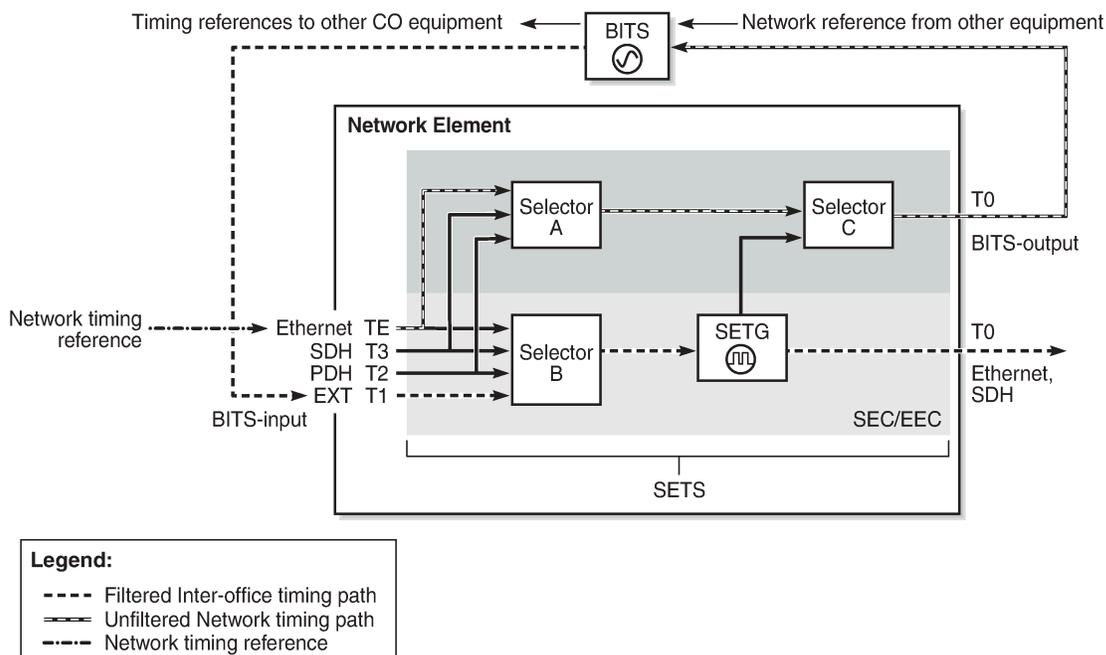
When configuring the priority order of the timing references with the **ref-order** command for unfiltered BITS output (T4), all reference sources are valid options, except the BITS input, which is excluded to avoid a timing loop. Because the same priority order is used for the SETG output (T0), the BITS input option must be set as the first (highest-priority) reference option.

Because both input and output clock pins are inside the physical RJ45 port for each BITS port, a custom cable is required to connect input and output ports to different equipment. See the 7705 SAR-18 Chassis Installation Guide, BITS Ports and Pinouts.

6.4.2 Line timing mode

Line timing from a synchronous port, such as a T1/E1 port or synchronous Ethernet port, provides the best synchronization performance through a synchronization distribution network. Line timing mode derives an 8 kHz clock from the framing of T1/E1, DS3/E3, and SONET/SDH signaling that can be used as an accurate reference between nodes in a network. Line timing mode is immune to any packet delay variation (PDV) occurring on Layer 2 or Layer 3 links.

On the 7705 SAR-M variants with T1/E1 ports, line timing is supported on the T1/E1 ports. Line timing is also supported on all RJ45 Ethernet ports and SFP ports on the 7705 SAR-M and on the following 7705 SAR-M modules:

- 2-port 10GigE (Ethernet) module
- 6-port SAR-M Ethernet module

On the 7705 SAR-X, line timing is supported on T1/E1 ports and Ethernet ports.

On the 7705 SAR-H and 7705 SAR-Hc, line timing is supported on all Ethernet ports. Line timing is also supported on the following 7705 SAR-H modules:

- 4-port SAR-H Fast Ethernet module
- T1/E1 ports of the 4-port T1/E1 and RS-232 Combination module

On the 7705 SAR-A variant with T1/E1 ports, line timing is supported on the T1/E1 ports. Line timing is also supported on all synchronous Ethernet ports on the 7705 SAR-A. Synchronous Ethernet is supported on the XOR ports (1 to 4), configured as either RJ45 ports or SFP ports. Synchronous Ethernet is also supported on SFP ports 5 to 8. Ports 9 to 12 do not support synchronous Ethernet and therefore do not support line timing.

On the 7705 SAR-Ax, line timing is supported on all Ethernet ports.

On the 7705 SAR-Wx, line timing is supported on all Ethernet RJ45 ports and SFP ports.

On the 7705 SAR-8 Shelf V2 and 7705 SAR-18, line timing is supported on the following adapter cards:

- 16-port T1/E1 ASAP Adapter card
- 32-port T1/E1 ASAP Adapter card
- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card (dual-rate and copper SFPs do not support synchronous Ethernet)
- 2-port 10GigE (Ethernet) Adapter card
- 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)
- 4-port DS3/E3 Adapter card
- 2-port OC3/STM1 Channelized Adapter card
- 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card
- 4-port OC3/STM1 Clear Channel Adapter card
- Packet Microwave Adapter card on ports that support synchronous Ethernet and on ports that support PCR

6.4.3 Adaptive Clock Recovery (ACR)

Adaptive Clock Recovery (ACR) is a timing-over-packet technology that transports timing information via periodic packet delivery over a pseudowire. ACR may be used when there is no other Stratum 1 traceable clock available.

ACR is supported on T1/E1 CES circuits on the following:

- 16-port T1/E1 ASAP Adapter card
- 32-port T1/E1 ASAP Adapter card
- 7705 SAR-M (variants with T1/E1 ports)
- 7705 SAR-A (variant with T1/E1 ports)
- T1/E1 ports of the 4-port T1/E1 and RS-232 Combination module
- T1/E1 ports on the 7705 SAR-X

ACR is not supported on DS1 or E1 channels that have CAS signaling enabled.

ACR is supported for Cpipe services. In addition, ACR is supported on MEF 8 Epipe services. The MEF 8 Epipe may be a TDM SAP to Ethernet SAP or a TDM SAP to spoke SDP. See the *7705 SAR Services Guide*, "MEF 8", for information about MEF 8.

There is no extra equipment cost to implement ACR in a network because this technique uses the packet arrival rate of a TDM pseudowire within the 7705 SAR to regenerate a clock signal. Additionally, the nodes in the network that are traversed between endpoints do not need special ACR capabilities. However, because the TDM pseudowire is transported over Layer 2 links, the packet flow is susceptible to PDV.

To achieve the best ACR performance, follow these recommendations:

- use a packet rate between 1000 pps and 4000 pps. Lower packet rates cause ACR to be more susceptible to PDV in the network.

- limit the number of nodes traversed between the source end and the ACR end of the TDM pseudowire

- enable QoS in the network with the TDM pseudowire enabled for ACR classified as NC (network control)

- maintain a constant temperature as much as possible, because temperature variations will affect the natural frequency on the internal oscillators in the 7705 SAR

- ensure that the network does not contain a timing loop when it is designed

6.4.3.1 ACR states

There are five potential ACR states:

- normal

- phase tracking

- frequency tracking

- holdover

- free-run

When a port's ACR state is normal, phase tracking, or frequency tracking, the recovered ACR clock is considered a qualified reference source for the SSU. If this reference source is being used, then transitions between any of these three states do not affect SSU operation.

When a port's ACR state is free-run or holdover, the recovered ACR clock is disqualified as a reference source for the SSU. If this reference source is being used, then transitions to either of these two states cause the SSU to drop the reference and switch to the next highest prioritized reference source. This can potentially be SSU holdover.

6.4.3.2 ACR statistics

The system collects statistics on all ACR-capable ports. ACR statistics detail how the digital phase locked loop (DPLL) is functioning in one or more ACR instances in the adapter card. ACR statistics assist with isolating a problem during degraded synchronization performance or with anticipating future issues.

Within the DPLL, there are two values that contribute to ACR statistics:

- DCO frequency

- input phase error of each 2-second update interval

The DCO is the digitally controlled oscillator that produces the regenerated clock signal. The input phase error is the correction signal that provides feedback to the DPLL to tune the DCO output. The input phase error should approach zero as the DPLL locks in to the source timing information and stabilizes the output.

The continuous 2-second updates to the output DCO frequency are directly applied as the clock output of the ACR instance. ACR statistics allow you to view the mean frequency and the standard deviation of the output DCO frequency.

During every 2-second update interval, the input phase error and the output DCO frequency are recorded. The input phase error mean, input phase error standard deviation, output DCO mean (Hz and ppb), and output DCO standard deviation are calculated every 60 seconds.

Entering a **show** CLI command on a port with ACR displays the mean and standard deviation values for the previous 60-second interval. A **show detail** command on the same port displays the previous 15 sets of 60-second intervals and a list of state and event counts. An SNMP MIB is also available with these statistics.

6.4.4 Differential Clock Recovery (DCR)

Differential Clock Recovery (DCR) is an alternative method to ACR to maintain the service clock across the packet network for a circuit emulated service. DCR is supported on:

- 16-port T1/E1 ASAP Adapter card
- 32-port T1/E1 ASAP Adapter card
- 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card (DS1/E1 channels)
- 4-port DS3/E3 Adapter card (clear channel DS3/E3 ports and DS1/E1 channels on channelized DS3 ports (E3 ports cannot be channelized)); DCR on DS1/E1 channels is supported only on the first three ports of the card
- 7705 SAR-M (variants with T1/E1 ports)
- 7705 SAR-A (variant with T1/E1 ports)
- T1/E1 ports of the 4-port T1/E1 and RS-232 Combination module
- T1/E1 ports on the 7705 SAR-X

In addition, DCR is supported between TDM SAPs and Ethernet SAPs and between TDM SAPs and spoke SDPs in a MEF 8 configuration for the above platforms, adapter cards, and modules. See the 7705 SAR Services Guide, "MEF 8", for information about MEF 8.

DCR is not supported on DS1 or E1 channels that have CAS signaling enabled.

DCR uses channel group 1 for timing recovery. If a T1 or E1 port is channelized, all TDM PWs that share the port use the timing recovered from channel group 1.

To enable DCR, the network must have a common clock between the routers performing the TDM-to-packet interworking function or between the two terminating SAPs or SAP/spoke SDP using MEF 8. The common clock can come from two PRC-traceable clocks or one clock that is made available to both ends, such as the transmitted clock of a SONET/SDH or synchronous Ethernet port.

In each direction, the service clock is compared to the common clock and the difference is encoded into the RTP header in the TDM PW overhead. At the other end of the network, the original service clock is reproduced by comparing the common clock to the frequency difference in the RTP header. Figure 12: Differential Clock Recovery on a network shows an example of a network using DCR.

Figure 12: Differential Clock Recovery on a network
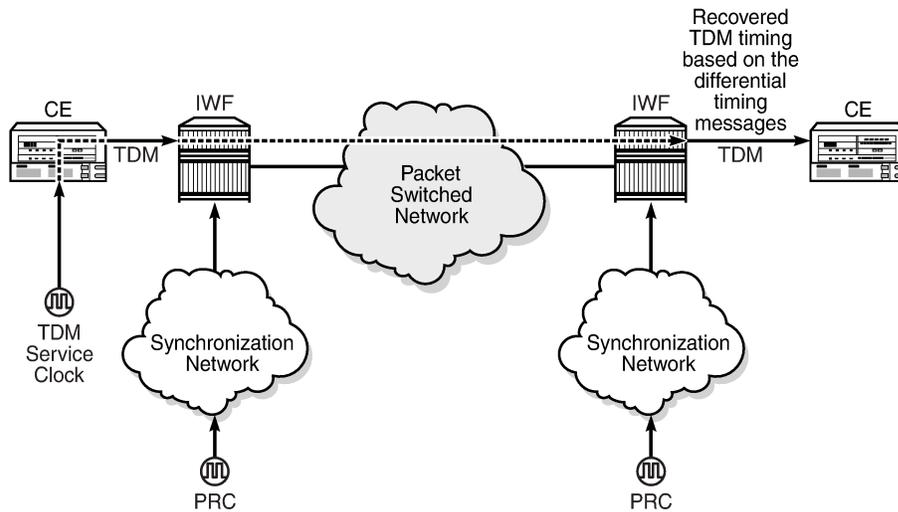
RTP headers are disabled by default and must be enabled for all circuit emulation services that require DCR. RTP must be enabled for the TDM PW that uses channel group 1. All channel groups on the same DS1 or E1 channel must be configured for the same mode of operation.

To achieve the best DCR performance, it is recommended that you use a Layer 1 network synchronization method to ensure the common clock has the best stability. If a timing-over-packet technique is used to transfer the common clock, then the number and type of nodes, the traffic profile, and the temperature variations will affect DCR synchronization performance. As well, a packet rate of at least 200 pps is recommended (up to 4000 pps is supported). Packet rates lower than 200 pps may affect system performance.

6.4.4.1 DCR frequencies

Each DS1, E1, DS3, or E3 circuit configured with DCR executes its own clock recovery from the packet stream. This allows each circuit to have an independent frequency.

Table 24: Supported timestamp frequencies for DCR-timed circuits lists the supported timestamp frequencies for each platform and adapter card.

Table 24: Supported timestamp frequencies for DCR-timed circuits

	Timestamp frequency (MHz)			
	103.68	77.76	25	19.44
16-port T1/E1 ASAP Adapter card		✓ (default)		✓
32-port T1/E1 ASAP Adapter card		✓ (default)		✓

	Timestamp frequency (MHz)			
	103.68	77.76	25	19.44
4-port OC3/STM1 / 1-port OC12/STM4 Adapter card		✓ (default)		
4-port DS3/E3 Adapter card		✓ (default)		
7705 SAR-M	✓ (default)	✓	✓	✓
7705 SAR-A	✓ (default)	✓	✓	✓
4-port T1/E1 and RS-232 Combination module	✓ (default)	✓	✓	✓
7705 SAR-X	✓ (default)	✓	✓	✓

The timestamp frequency is configured at the adapter card level and is used by all DCR ports or channels on the supporting platforms and cards. Both ends of a TDM pseudowire using DCR must be running the same frequency. If a network contains different types of equipment using DCR, a common frequency must be selected that is supported by all equipment.

DCR complies with published jitter and wander specifications (G.823, G.824, and G.8261) for traffic interfaces under typical network conditions and for synchronous interfaces under specified packet network delay, loss, and delay variance (jitter) conditions.

6.4.5 Serial clock transport (DCR serial)

A **dcr-serial** parameter option is available on the 12-port Serial Data Interface card, version 3, to support the SAToP serial virtual channel (vc) type of Cpipe. The **dcr-serial** option can be configured using the **serial>clock-source** command; it is only supported on synchronous RS-232 and RS-530 interfaces. See the 7705 SAR Interface Configuration Guide, "Serial Commands", for more information about how to configure DCR serial. See the *7705 SAR Services Guide*, "SAToP Serial", for information about SAToP serial.

During the normal transport of serial data traffic across a 7705 SAR IP/MPLS network, the time reference used to clock the data in/out of the 7705 SAR to the end device is based on the 7705 SAR system clock.

Some encryption applications, however, require both end devices on an encrypted link to run off the same time reference. To meet this requirement, the **dcr-serial** option is used to transport the system clock but only in a single direction: from the DTE-designated port of a SAToP serial Cpipe to the DCE-designated port at the other end. The source of the service clock is referenced to the Rx Clk signal of the DTE port on the 12-port Serial Data Interface card, version 3. One end of the a SAToP serial Cpipe must be set to DTE while the other end is set to DCE.

Note:

- Only one clock can be transported per port.

- The clock recovered by DCR serial is suitable only for clocking data into the attached device, not as a source of network synchronization.

- The input frequency clock tolerance must within 4.5% of the configured port rate.

- Although DCR serial is supported on 600 b/s port speeds, clock deviations from a nominal 600 b/s port speed are not supported. This applies to both RS-232 and RS-530 ports.

- There can be a maximum of 12 DCR serial timing instances per 12-port Serial Data Interface card, version 3.

6.4.6 Proprietary Clock Recovery (PCR)

PCR is a copper synchronous Ethernet-based, timing-over-packet technology. It is supported on the Packet Microwave Adapter card on the two copper RJ45 synchronous Ethernet 1000Base-T Microwave Awareness (MWA) ports (ports 1 and 2) and on a copper SFP Ethernet port (ports 3 and 4).

There is no CLI configuration requirement for PCR; it is turned on automatically when a microwave link is enabled on an MWA RJ45 port or on a copper SFP Ethernet port (ports 3 and 4).

> **Note:** On the MPR-e side, PCR requires that the MAC address of the 7705 SAR-8 Shelf V2 or 7705 SAR-18 be configured on the MPR-e radio that is connected to the 7705 SAR-8 Shelf V2 or 7705 SAR-18 chassis. See the latest version of the MPR-e user manual for the required information.

PCR provides the same frequency recovery capability as standard-based copper synchronous Ethernet without having to endure a traffic hit whenever a synchronous source switching occurs. See Figure 13: Proprietary Clock Recovery.

Figure 13: Proprietary Clock Recovery
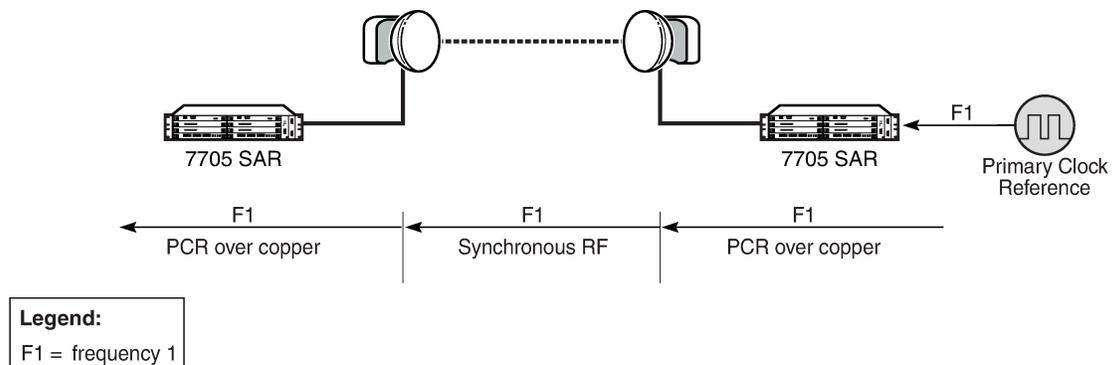
By running PCR between the MPR-e radio and the MWA port, frequency synchronization can be delivered in either direction. With standard-based copper synchronous Ethernet, there is a traffic hit every time a clock source change occurs on a 7705 SAR-8 Shelf V2 or 7705 SAR-18 because the 7705 SAR-8 Shelf V2 or 7705 SAR-18 and the MPR-e radio to which it is connected must bring down the Ethernet link MAC layer before it can renegotiate and reverse the master and slave clock role. This MAC layer renegotiation affects the data plane and the signaling and routing plane. All MPLS signaling links and the label switched path (LSP) are taken down during the renegotiation process; the routing signaling advertises the down state of the link throughout the network.

However, with PCR running on the microwave link, the physical layer transmit clock on a copper synchronous Ethernet port on the Packet Microwave Adapter card is always set to master. The reversal of the clock role only occurs at the PCR "layer". This means that a synchronous source change does not disrupt the data plane and the signaling and routing plane on the 7705 SAR-8 Shelf V2 or 7705 SAR-18.

6.4.7 IEEE 1588v2 PTP

> **Note:** The IEEE 1588 Working Group has introduced the terms timeTransmitter and timeReceiver as alternatives to the former master/slave terminology. This document has been updated with these new terms.

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard *1588 2008*.

PTP can be deployed as an alternative timing-over-packet option to ACR. PTP provides the capability to synchronize network elements to a Stratum-1 clock or primary reference clock (PRC) traceable source over a network that may or may not be PTP-aware. PTP has several advantages over ACR. It is a standards-based protocol, has lower bandwidth requirements, can transport both frequency and time, and can potentially provide better performance.

There are five basic types of PTP devices, as listed below:

- ordinary clock (timeTransmitter or timeReceiver)
- boundary clock
- end-to-end transparent clock
- peer-to-peer transparent clock
- management node

Table 25: IEEE 1588v2 PTP support per fixed platform lists the types of PTP support on each fixed platform; Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 lists the types of PTP support on each adapter card for the 7705 SAR-8 Shelf V2 and the 7705 SAR-18.

> **Note:**
> - All clock types, with the exception of transparent clock, support PTP messaging using UDP/IPv4 or UDP/IPv6.
> - IPv6 messaging is supported on all platforms and cards listed in Table 25: IEEE 1588v2 PTP support per fixed platform and Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 .
> - Boundary clocks support dual mode; that is, the clock can be configured for both IPv4 and IPv6. Dual mode is not supported on ordinary clocks; the clock can only be configured for IPv4 or IPv6.

Table 25: IEEE 1588v2 PTP support per fixed platform

Sync type	PTP clock type	7705 SAR-A 7705 SAR-Ax 7705 SAR-H 7705 SAR-Hc 7705 SAR-M 7705 SAR-Wx 7705 SAR-X
Freq	Ordinary timeReceiver	✓
	Boundary clock	✓
	End-to-end transparent clock	✓
	Ordinary timeTransmitter	✓
Time of day/ phase	Ordinary timeReceiver	✓
	Boundary clock	✓
	End-to-end transparent clock	✓ [1]
	Ordinary timeTransmitter	✓ [2]

Notes:

1. The 2-port 10GigE (Ethernet) module supports transparent clock functionality when installed in the 7705 SAR-M

2. Only supported on the 7705 SAR-H with a GPS Receiver module and 7705 SAR-Wx variants with a GPS RF port.

All the platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform support one ordinary timeReceiver clock, ordinary timeTransmitter clock, or boundary clock. The platforms also support an additional PTP clock for transparent clock functionality.

Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18

Sync type	PTP clock type	6-port Ethernet 10Gbps Adapter Card	8-port Gigabit Ethernet Adapter Card	Packet Microwave Adapter Card	2-port 10GigE (Ethernet) Adapter Card	10-port 1GigE/ 1-port 10GigE X-Adapter Card [1]
Freq	Ordinary timeReceiver	✓	✓	✓	✓	✓
	Boundary clock	✓	✓	✓	✓	✓

Sync type	PTP clock type	6-port Ethernet 10Gbps Adapter Card	8-port Gigabit Ethernet Adapter Card	Packet Microwave Adapter Card	2-port 10GigE (Ethernet) Adapter Card	10-port 1GigE/ 1-port 10GigE X-Adapter Card [1]
	End-to-end transparent clock					
	Ordinary timeTransmitter	✓	✓	✓	✓	✓
Time of day/ phase	Ordinary timeReceiver	✓	✓	✓	✓	✓
	Boundary clock	✓	✓	✓	✓	✓
	End-to-end transparent clock					
	Ordinary timeTransmitter [2]	✓	✓	✓	✓	✓

Notes:

1. Not supported on the 7705 SAR-8 Shelf V2.

2. Supported on chassis with an active GNSS Receiver card.

The 7705 SAR-8 Shelf V2 supports up to six ordinary timeReceiver clocks, ordinary timeTransmitter clocks, or boundary clocks. The 7705 SAR-18 supports up to eight ordinary timeReceiver clocks, ordinary timeTransmitter clocks, or boundary clocks.

Each of the cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 supports one PTP clock.

A nodal clock is equipped in each CSM on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 or directly on the fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform. Up to two PTP ordinary or boundary clocks can be configured per node as references to the nodal clock.

Each PTP timeReceiver clock can be configured to receive timing from up to two PTP timeTransmitter clocks in the network.

6.4.7.1 Best TimeTransmitter Clock Algorithm

Each timeTransmitter clock has its own configuration for IP address, packet rate, and messaging timeouts, and for statistics, alarms, and events. Each available timeTransmitter clock advertises its presence and information using Announce messages. If both timeTransmitter clocks are available, the timeReceiver clock uses the Best TimeTransmitter Clock Algorithm (BTCA) to dynamically compare the information in the Announce messages of each timeTransmitter clock to determine to which of the two timeTransmitter clocks it should synchronize. This timeTransmitter clock is known as the best timeTransmitter. After the timeReceiver clock has determined which is the best timeTransmitter, it can begin to negotiate with it for unicast synchronization communication.

The configured setting for the **profile** command determines the precedence order for selecting the best timeTransmitter clock algorithm. The 7705 SAR supports the following profile settings: **ieee1588-2008**,

itu-telecom-freq, **g8275dot1-2014**, **g8275dot2-2016**, **iec-61850-9-3-2016**, and **c37dot238-2017**. For information about the **g8275dot1-2014** and **g8275dot2-2016** profile parameters, see ITU-T G.8275.1 and G.8275.2. For information about the **iec-61850-9-3-2016** and **c37dot238-2017** profile parameters, see IEC/IEEE 61850-9-3 and C37.238-2017.

If the **profile** setting for the clock is **ieee1588-2008**, **iec-61850-9-3-2016**, or **c37dot238-2017**, the precedence order for the best timeTransmitter selection algorithm is as follows:

- priority1 (user-configurable on the timeTransmitter clock side)
- clock class
- clock accuracy
- PTP variance (offsetScaledLogVariance)
- priority2 (user-configurable on the timeTransmitter clock side)
- clock identity
- distance (number of boundary clocks)

If the **profile** setting for the clock is **itu-telecom-freq** (ITU-T G.8265.1 profile), the precedence order for the best timeTransmitter selection algorithm is as follows:

- clock class
- peer ID

If the **profile** setting for the clock is **g8275dot1-2014** or **g8275dot2-2016**, the precedence order for the best timeTransmitter selection algorithm is as follows if the grandmaster clock is connected to a primary reference time clock (PRTC) in locked mode:

- clock class
- clock accuracy
- PTP variance (offsetScaledLogVariance)
- priority2 (user-configurable on the timeTransmitter clock side)
- localPriority
- steps removed from the grandmaster
- port identities
- port numbers

If the **profile** setting for the clock is **g8275dot1-2014** or **g8275dot2-2016**, the precedence order for the best timeTransmitter selection algorithm is as follows if the grandmaster clock is in holdover and out of holdover specification, or is without a time reference since startup:

- clock class
- clock accuracy
- PTP variance (offsetScaledLogVariance)
- priority2 (user-configurable on the timeTransmitter clock side)
- localPriority
- clock identity
- steps removed from the grandmaster
- port identities

- port numbers

The following figure shows an example of the messaging sequence between the PTP timeReceiver clock and the two PTP timeTransmitter clocks.

Figure 14: Messaging sequence between the PTP timeReceiver clock and PTP timeTransmitter clocks
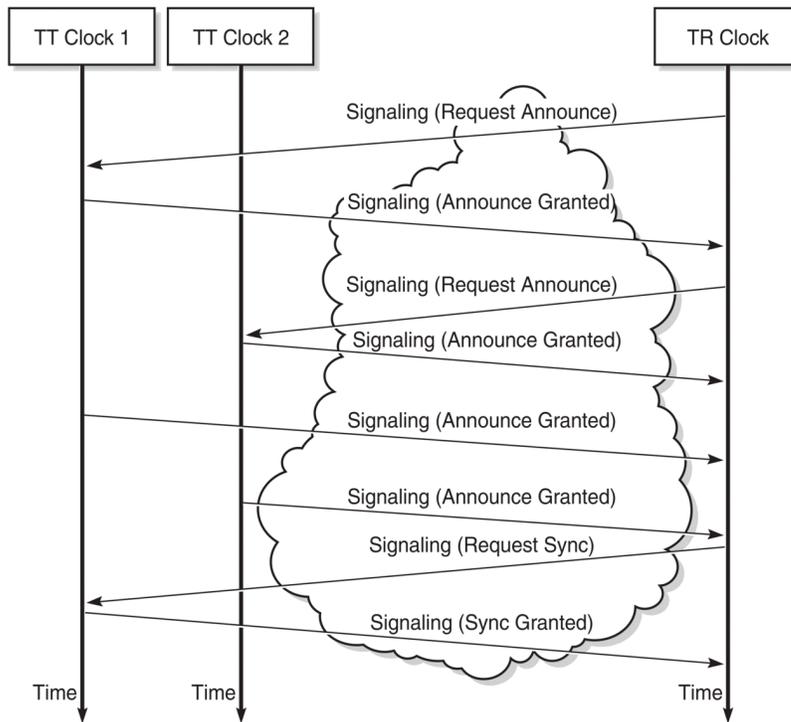
6.4.7.2 PTP clock synchronization

The IEEE 1588v2 standard synchronizes the frequency and time from a timeTransmitter clock to one or more timeReceiver clocks over a packet stream. This packet-based synchronization can be over UDP/IP or Ethernet and can be unicast (for IP) or multicast (for Ethernet). For UDP/IP, both IPv4 and IPv6 unicast mode with unicast negotiation is supported.

As part of the basic synchronization timing computation, a number of event messages are defined for synchronization messaging between the PTP timeReceiver clock and PTP timeTransmitter clock. A one-step or two-step synchronization operation can be used, with the two-step operation requiring a follow-up message after each synchronization message. Currently, only one-step operation is supported when the 7705 SAR is a timeTransmitter clock; PTP frequency and time can be recovered from both one-step and two-step operation when the 7705 SAR is acting as a timeReceiver or boundary clock.

For IPv4, the two-step operation is optional. For IPv6, the two-step operation is a mandatory requirement for the 7705 SAR.

> **Note:** Two-step operation does not apply if PTP packets are routed over a physical port on the 7705 SAR-X or on the 6-port Ethernet 10Gbps Adapter card.

In one-step operation, a timestamp is inserted in the synchronization message when the packet is transmitted to the timeReceiver clock. In two-step operation, the timestamp is sent in the follow-up message. If the timestamp is changed in the synchronization message, the checksum field is recomputed. Because the checksum field is a mandatory field for IPv6 (optional for IPv4), the 7705 SAR requires the timestamp to be sent separately to avoid potential checksum corruption in the packet.

During startup, the PTP timeReceiver clock receives the synchronization messages from the PTP timeTransmitter clock before a network delay calculation is made. Before any delay calculation, the delay is assumed to be zero. A drift compensation is activated after a number of synchronization message intervals occur. The expected interval between the reception of synchronization messages is user-configurable.

The basic synchronization timing computation between the PTP timeReceiver clock and PTP best timeTransmitter is illustrated in the following figure. This figure illustrates the offset of the timeReceiver clock referenced to the best timeTransmitter signal during startup.

Figure 15: PTP timeReceiver clock and timeTransmitter clock synchronization timing computation
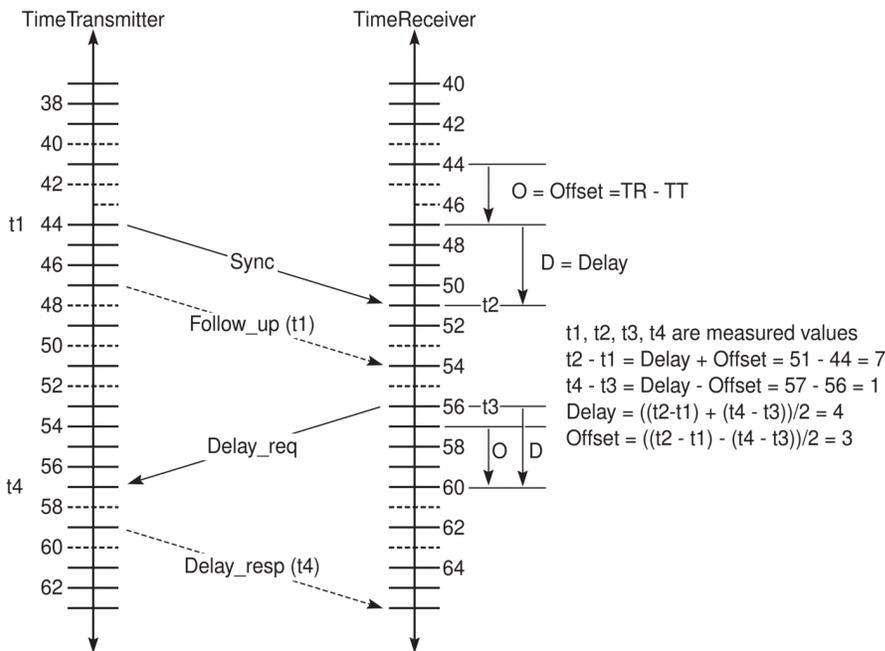
6.4.7.3 Performance considerations

Although IEEE 1588v2 can be used on a network that is not PTP-aware, the use of PTP-aware network elements (boundary clocks) within the packet switched network improves synchronization performance by reducing the impact of PDV between the grandmaster clock and the timeReceiver clock.

Note:

- The grandmaster clock is the timeTransmitter clock for the network. The best timeTransmitter clock is the clock that the timeReceiver clock selects as its timeTransmitter. For example, the timeReceiver clock's best timeTransmitter clock may be a boundary clock, which is connected to a grandmaster clock.

- A 7705 SAR equipped with a GNSS receiver can function as a grandmaster clock.

The performance objective is to meet the synchronization interface maximum time interval error (MTIE) mask. Similar to ACR, the number of factors with the PSN contributes to how well PTP can withstand, and still meet, those requirements.

6.4.7.4 PTP capabilities

PTP messages are supported via IPv4 unicast with a fixed IP header size or via IPv6.

PTP messaging is supported on network interfaces. If a node loopback address is used as the source interface for 1588 packets, the packets can ingress any network IP interface on the router. If the source interface is associated with a physical port, packets must be sent to the interface on that port.

PTP messaging is also supported on IES interfaces for access ports.

The 7705 SAR can also forward IPv4-encapsulated PTP messages over BGP-LU routes for frequency synchronization. The following profiles are supported for these messages: **ieee1588-2008**, **itu-telecom-freq**, and **g8275dot2-2016**.

The following table describes the supported message rates for timeReceiver and timeTransmitter states for IP-encapsulated PTP traffic, based on the profile configured. The ordinary clock can be either in the timeReceiver or timeTransmitter state. The boundary clock can be in both of these states.

Table 27: Rates for IP-encapsulated PTP messages

Message/rate		ieee1588-2008	itu-telecom-freq	g8275dot1-2014 g8275dot2-2016
Announce	Minimum rate	1 per 16 seconds	1 per 16 seconds	1 per 16 seconds
	Maximum rate	8 per second	8 per second	8 per second
	Default rate	1 per 2 seconds	1 per 2 seconds	8 per second
Sync and Delay	Minimum rate[1]	64 per second	64 per second	16 per second
	Maximum rate	128 per second	128 per second	128 per second
	Default rate	64 per second	64 per second	16 per second

Note:

1. In the timeTransmitter clock state, the minimum rate granted is 1 per 16 seconds if requested by the timeReceiver clock.

See Table 30: Rates for Ethernet-encapsulated PTP messages for the supported message rates for Ethernet-encapsulated PTP traffic.

State and statistics data for each timeTransmitter clock are available to assist in the detection of failures or unusual situations.

The PTP algorithm is able to recover the clock using both the upstream and downstream directions in both ordinary timeReceiver and boundary clock modes. The ability to perform bidirectional recovery improves the performance of networks where the upstream and downstream load is not symmetrical.

The Bell Labs algorithm looks at the PTP packet exchange in both directions between the timeTransmitter and timeReceiver. There can be more packet delay variation in one direction if there is a high utilization rate or congestion in that direction. The algorithm assesses the stability and reliability of the packet exchange in each direction and assigns weight values based on the results. The system gives preference to frequency synchronization from the direction with a higher weight value. The weight values change dynamically and can be viewed with detailed PTP show commands.

6.4.7.5 PTP ordinary timeReceiver clock for frequency

The PTP ordinary clock with timeReceiver capability on the 7705 SAR provides an option to reference a Stratum-1 traceable clock across a packet switched network. The recovered clock can be referenced by the internal SSU and distributed to all slots and ports.

The following figure shows a PTP ordinary timeReceiver clock network configuration.

Figure 16: TimeReceiver clock
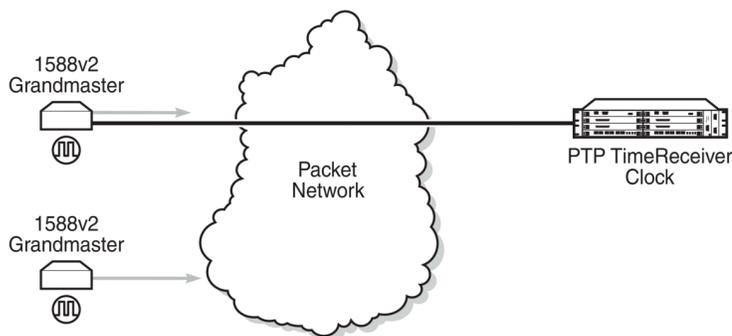
The PTP timeReceiver capability is implemented on the Ethernet ports of the platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform and on the cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 .

The 7705 SAR-8 Shelf V2 can support up to six timeReceiver clocks and the 7705 SAR-18 can support up to eight timeReceiver clocks.

All other fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform can support up to two PTP clocks when one of those clock types is configured as transparent; otherwise, they support only one timeReceiver clock.

Each timeReceiver clock can provide a separate frequency reference to the SSU.

The following figure shows the operation of an ordinary PTP clock in timeReceiver mode.

Figure 17: Ordinary timeReceiver clock operation
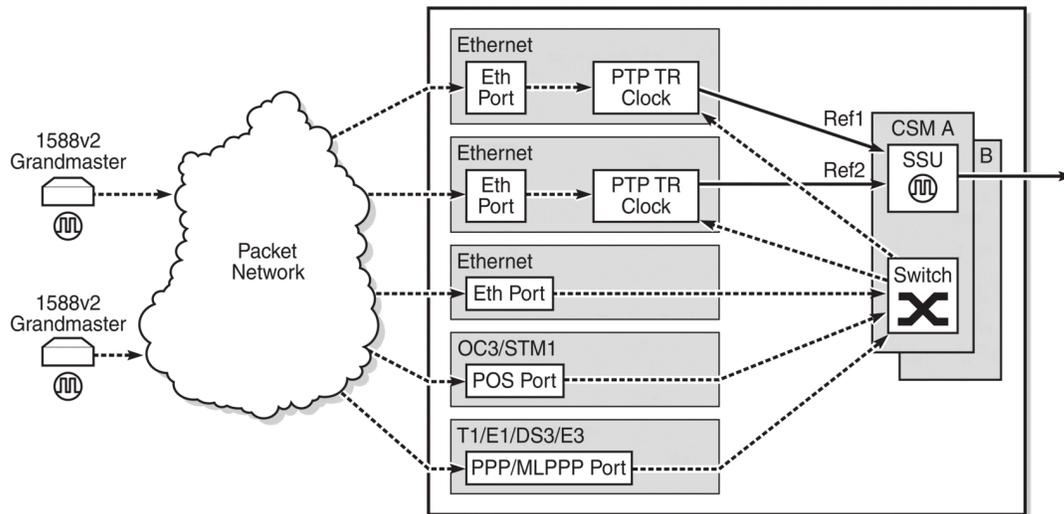
Each PTP ordinary timeReceiver clock is configured for a specific slot where the card (see Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18) or Ethernet port (see Table 25: IEEE 1588v2 PTP support per fixed platform) performs the timeReceiver function. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-Wx, this slot is always 1/1. On the 7705 SAR-X, this slot is always either 1/2 or 1/3. When the 7705 SAR-M is receiving PTP packets on the 2-port 10GigE (Ethernet) module, its PTP clock continues to use slot 1/1. Each timeReceiver is also associated with an IP interface on a specific port, adapter card, or loopback address for the router; however, the IP interface configured on a 2-port 10GigE (Ethernet) module cannot be associated with a timeReceiver clock.

For best performance, the network should be designed so that the IP messaging between the timeTransmitter clock and the timeReceiver clock ingresses and egresses through a port where the timeReceiver is configured. If the ingress and egress flow of the PTP messages is via a different port or adapter card on the 7705 SAR, then the packets are routed through the fabric to the Ethernet card with the PTP timeReceiver.

It is possible that the PTP IP packets may be routed through another Ethernet port/VLAN, OC3/STM1 or OC12/STM4 clear channel POS, OC3/STM1 or OC12/STM4 channelized MLPPP, DS3/E3 PPP, or DS1/E1 MLPPP. The PTP timeReceiver performance may be slightly worse in this case because of the extra PDV experienced through the fabric. Packets are routed this way only if the clock is configured with a loopback address. If the clock is configured with an address tied to a physical port, the packets arrive on that physical port as described above.

6.4.7.6 PTP ordinary timeTransmitter clock for frequency

The 7705 SAR supports the PTP ordinary clock in timeTransmitter mode. Normally, a 1588v2 grandmaster is used to support many timeReceivers and boundary clocks in the network. In cases where only a small number of timeReceivers and boundary clocks exist and only frequency is required, a PTP integrated timeTransmitter clock can greatly reduce hardware and management costs to implement PTP across the network. It also provides an opportunity to achieve better performance by placing a timeTransmitter clock deeper into the network, as close to the timeReceiver clocks as possible.

The following figure shows a PTP timeTransmitter clock network configuration.

Figure 18: PTP timeTransmitter clock
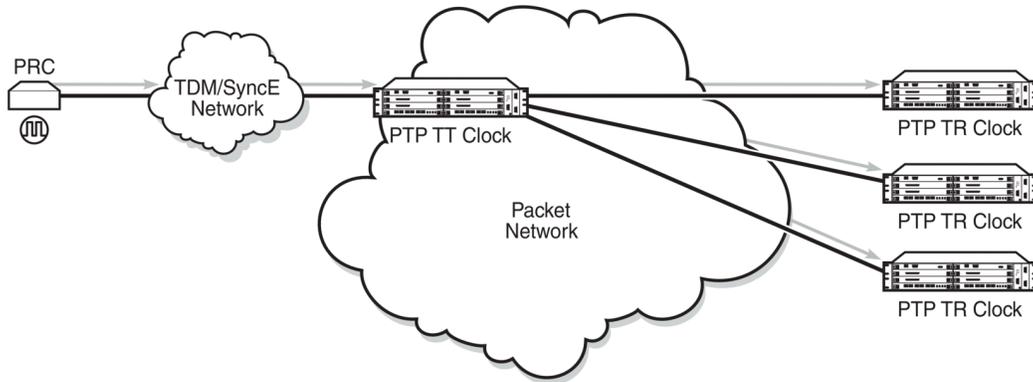
The PTP timeTransmitter clock capability is implemented on the Ethernet ports of the platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform and on the cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 .

The 7705 SAR-8 Shelf V2 can support up to six timeTransmitter clocks and the 7705 SAR-18 can support up to eight timeTransmitter clocks. The fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform can each support one timeTransmitter clock.

The following figure shows the operation of an ordinary PTP clock in timeTransmitter mode.

Figure 19: Ordinary timeTransmitter clock operation
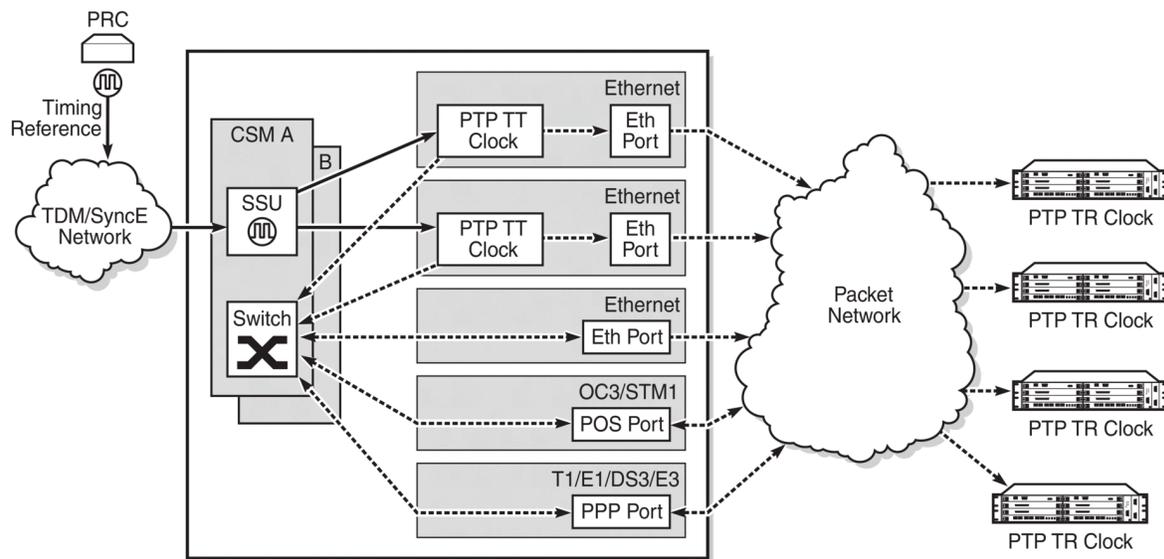
Each PTP timeTransmitter clock is configured for a specific slot where the card (see Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18) or Ethernet port (see Table

25: IEEE 1588v2 PTP support per fixed platform) performs the timeTransmitter function. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-Wx, this slot is always 1/1. On the 7705 SAR-X, this slot is always either 1/2 or 1/3. When the 7705 SAR-M is receiving PTP packets on a 2-port 10GigE (Ethernet) module, its PTP clock continues to use slot 1/1. Each timeTransmitter is also associated with an IP interface on a specific port, adapter card, or loopback address for the router; however, the IP interface configured on a 2-port 10GigE (Ethernet) module cannot be associated with a timeTransmitter clock. All packets that ingress or egress through a port where the timeTransmitter is configured are routed to their destination via the best route as determined in the route table.

Each timeTransmitter clock can peer with up to 50 timeReceivers or boundary clocks. The IP addresses of these peers can be statically configured via CLI or dynamically accepted via PTP signaling messages. A statically configured peer may displace a dynamic peer on a particular PTP port. If there are fewer than 50 peers, then that dynamic peer can signal back and be granted a different PTP port instance.

6.4.7.7 PTP boundary clock for frequency

The 7705 SAR supports boundary clock PTP devices in both timeTransmitter and timeReceiver states. IEEE 1588v2 can function across a packet network that is not PTP-aware; however, the performance may be unsatisfactory and unpredictable. PDV across the packet network varies with the number of hops, link speeds, usage rates, and the inherent behavior of the routers. By using routers with boundary clock functionality in the path between the grandmaster clock and the timeReceiver clock, one long path over many hops is split into multiple shorter segments, allowing better PDV control and improved timeReceiver performance. This allows PTP to function as a valid timing option in more network deployments and allows for better scalability and increased robustness in specific topologies, such as rings.

Boundary clocks can simultaneously function as a PTP timeReceiver of an upstream grandmaster (ordinary clock) or boundary clock, and as a PTP timeTransmitter of downstream timeReceivers (ordinary clocks) or boundary clocks. The following figure shows the operation of a boundary clock.

Figure 20: Boundary clock
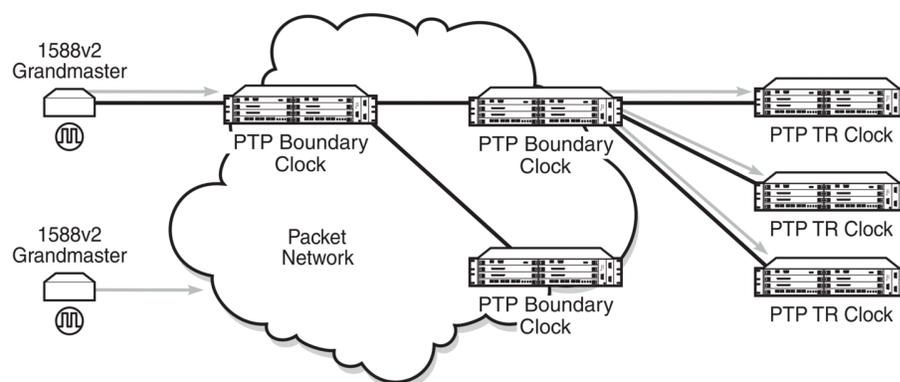
The PTP boundary clock capability is implemented on the Ethernet ports of the platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform and on the cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 .

The 7705 SAR-8 Shelf V2 can support up to six boundary clocks and the 7705 SAR-18 can support up to eight boundary clocks. The fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform can each support one boundary clock.

Each PTP boundary clock is configured for a specific slot where the card (see Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18) or Ethernet port (see Table 25: IEEE 1588v2 PTP support per fixed platform) performs the boundary clock function. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-Wx, this slot is always 1/1. On the 7705 SAR-X, this slot is always either 1/2 or 1/3. When the 7705 SAR-M is receiving PTP packets on a 2-port 10GigE (Ethernet) module, its PTP clock continues to use slot 1/1. Each boundary clock is also associated with a loopback address for the router; however, the IP interface configured on a 2-port 10GigE (Ethernet) module cannot be associated with a boundary clock.

Each boundary clock can be peered with up to 50 timeReceivers, boundary clocks, or grandmaster clocks. The IP addresses of these peers can be statically configured via CLI or dynamically accepted via PTP signaling messages. A statically configured peer may displace a dynamic peer on a particular PTP port. If there are fewer than 50 peers, that dynamic peer can signal back and be granted a different PTP port instance.

The following figure shows an example of boundary clock operation.

Figure 21: Boundary clock operation
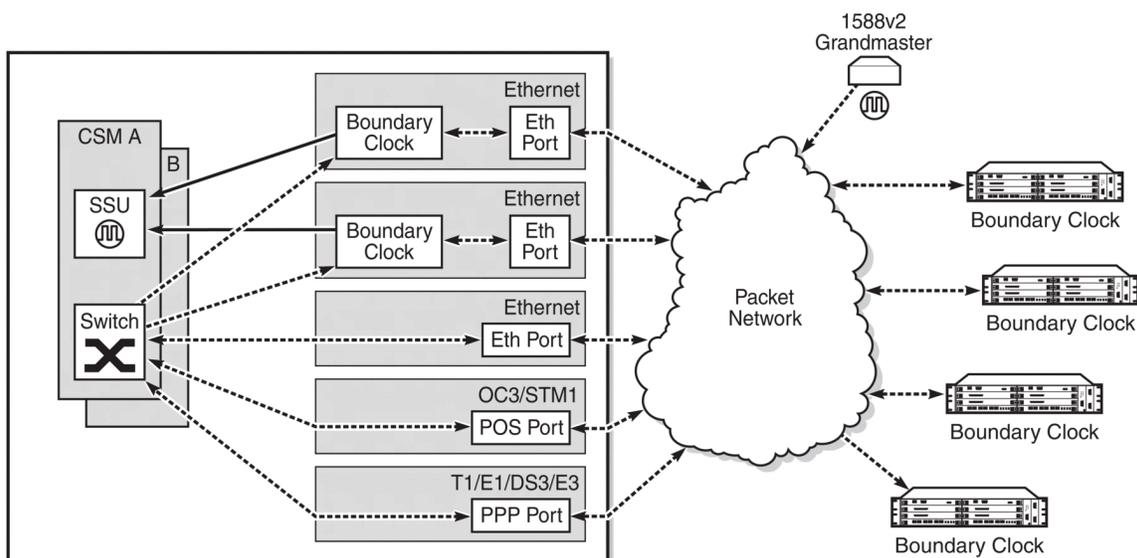
21309

6.4.7.8 PTP ordinary timeReceiver clock for time of day/phase recovery

The following equipment supports PTP timeReceiver clock for time of day/phase recovery:

- all fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform
- all cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18

The 7705 SAR can receive and extract time of day/phase recovery from a 1588 grandmaster clock or boundary clock and transmit the recovered time of day/phase signal to an external device such as a base station through an external time of day port, where available. The PTP timeReceiver clock can be used as a reference for the router system time clock, providing high-accuracy OAM timestamping and measurements for the 7705 SAR chassis.

On the 7705 SAR-8 Shelf V2 CSMv2, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-M, and 7705 SAR-X, transmission is through the ToD port with a 1 pulse/s output signal that is phase-aligned with other routers that are similarly time of day/phase synchronized. An RS-422 serial interface within the ToD port connector communicates the exact time of day of the rising edge of the 1 pulse/s signal. The serial interface on the ToD out port and the ToD in port on the CSMv2 are currently not supported; therefore, the 7705 SAR-8 Shelf V2 does not support Time of Day messages.

On the 7705 SAR-H, transmission is through the IRIG-B Out port. An RJ45 interface is used for the IRIG-B Out port to communicate the exact time of day by the rising edge of the 1 pulse/s signal, an IRIG-B000 unmodulated time code signal, and an IRIG-B12X modulated time code signal.

On the 7705 SAR-H, the Time of Day message output is only available when the router is configured with an active IP PTP timeReceiver clock or boundary clock. For all other routers, the Time of Day message output is available when the router is configured with an active IP PTP timeReceiver clock or boundary clock or when Time of Day is recovered from an Ethernet PTP clock or integrated GNSS.

The following table lists the 1 pulse/s signal (1pps) support and Time of Day messaging support per platform.

Table 28: 1pps/ToD message support

Platform	1pps out	ToD messages out	1pps in	ToD messages in
7705 SAR-8 Shelf V2 CSMv2	Yes	No	No	No
7705 SAR-A	Yes	Yes for IP PTP Yes for Ethernet PTP	No	No
7705 SAR-Ax	Yes	Yes for IP PTP Yes for Ethernet PTP	No	No
7705 SAR-H	Yes	Yes for IP PTP No for Ethernet PTP	No	No
7705 SAR-M	Yes	Yes for IP PTP Yes for Ethernet PTP	No	No
7705 SAR-X	Yes	Yes for IP PTP Yes for Ethernet PTP	No	No

The following table describes the format of the ToD message.

Table 29: ToD messages

Byte offset	Length	Field name	Description
0	4	Second time of week	The GPS time of week, in seconds
4	4	Reserved	n/a

Byte offset	Length	Field name	Description
8	2	Week	The GPS week (GPS time)
10	1	LeapS	Leap seconds (GPS-UTC)
11	1	1PPS status	The 1pps signal value: [1] • 0x00 – 1pps is in a normal state and is time-traceable to PRTC and frequency-traceable to PRS/PRC • 0x02 – 1pps is not traceable
12	1	TAcc	The jitter level of 1PPS. This field is currently not in use.
13	1	Reserved	n/a
14	1	Reserved	n/a
15	1	Reserved	n/a

Note:

1. Enhanced ToD 1pps values are not supported on the 7705 SAR-H.

For incoming IEEE 1588 packets, the destination IP address is the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, or 7705 SAR-X loopback address. The ingress interface can be an SFP Ethernet port on the faceplate of the chassis, an RJ45 port on the faceplate of the chassis, or a port on an installed module.

Each PTP timeReceiver clock can be configured to receive timing from up to two PTP timeTransmitter clocks in the network. If both timeTransmitter clocks are available, the timeReceiver clock uses default BTCA to determine which of the two timeTransmitter clocks it should synchronize.

PTP messaging between the PTP timeTransmitter clock and PTP timeReceiver clock is done over UDP/IP using IPv4 unicast mode with a fixed IP header size or using IPv6. Unicast negotiation is supported. Each PTP instance supports up to 128 synchronization messages per second.

PTP recovered time accuracy depends on the delay of the forward path and the reverse path being symmetrical. It is possible to correct for known path delay asymmetry by using the **ptp-asymmetry** command for PTP packets destined for the local timeReceiver clock or downstream PTP timeReceiver clock.

6.4.7.9 PTP boundary clock for time of day/phase recovery

The following equipment supports PTP boundary clock capability for time of day/phase recovery:

• all fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform

• all cards listed in Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18

The 7705 SAR-8 Shelf V2 can support up to six boundary clocks and the 7705 SAR-18 can support up to eight boundary clocks. The fixed platforms can each support one boundary clock. PTP boundary clocks that recover time of day/phase from a grandmaster clock or another boundary clock can be used as a

reference for the router system time clock, providing high-accuracy OAM timestamping and measurements for the 7705 SAR chassis.

Each PTP boundary clock for time of day/phase is configured for a specific slot where the adapter card or port performs the boundary clock function. On fixed platforms, with the exception of the 7705 SAR-X, this slot is always 1/1. On the 7705 SAR-X, this slot is always either 1/2 or 1/3. Each boundary clock is also associated with a loopback or system address for the router.

6.4.7.10 PTP end-to-end transparent clock for time of day/phase recovery

PTP end-to-end transparent clock for time of day/phase recovery is supported on the following:

- the fixed platforms listed in Table 25: IEEE 1588v2 PTP support per fixed platform
- 2-port 10GigE (Ethernet) module

Transparent clock functionality is supported for PTP packets over UDP/IP over Ethernet (with and without VLAN tags).

For high-accuracy 1588 PTP clock recovery, timestamping of incoming and outgoing messages should be done as close to ingress and egress as possible when the 7705 SAR is acting as a 1588 transparent clock. Edge timestamping is performed on all packets from all Ethernet ports, including SFP and RJ45 ports on the faceplate of the chassis or a port on an installed module.

PTP recovered time accuracy depends on the delay of the forward path and the reverse path being symmetrical. It is possible to correct for known path delay asymmetry by using the **ptp-asymmetry** command to configure an asymmetry delay setting in nanoseconds per direction for each edge.

To enable transparent clock processing at the node level, configure a PTP clock with the **transparent-e2e** clock type (using the **clock-type** command). Deconfiguring such a PTP clock disables transparent clock processing.

6.4.7.11 PTP timeTransmitter clock for time of day/phase distribution

PTP timeTransmitter clock capability for time of day/phase distribution is implemented on the following platforms:

- 7705 SAR-H with a GPS Receiver module
- 7705 SAR-Wx variants with a GPS RF port
- 7705 SAR-8 Shelf V2 with a GNSS Receiver card
- 7705 SAR-18 with a GNSS Receiver card

Time of day input must be enabled using the **use-node-time** command before the node can be used as a PTP grandmaster clock. GNSS must also be the active system time reference for nodes that are being used as a grandmaster clock. When the **use-node-time** command is enabled, the PTP timeTransmitter clock uses the system time as a source of PTP time and can be used for time of day/phase distribution. When the **use-node-time** command is disabled, the PTP timeTransmitter clock can be used for frequency only.

6.4.7.12 PTP clock redundancy

Each PTP timeReceiver clock can be configured to receive timing from up to two PTP timeTransmitter clocks. If two PTP timeTransmitter clocks are configured, and if communication to the best timeTransmitter

is lost or if the BTCA determines that the other PTP timeTransmitter clock is better, then the PTP timeReceiver clock switches to the other PTP timeTransmitter clock.

For a redundant or simple CSM configuration on the 7705 SAR-8 Shelf V2 and 7705 SAR-18, a maximum of two PTP timeReceiver clocks can be configured as the source of reference (ref1 and ref2) to the SSU. If a failure occurs between the PTP timeReceiver clock and the timeTransmitter clock, the SSU detects that ref1 or ref2 is unavailable and automatically switches to the other reference source. This switching provides PTP hot redundancy for hardware failures (on the 6-port Ethernet 10Gbps Adapter card, 8-port Gigabit Ethernet Adapter card, 10-port 1GigE/1-port 10GigE X-Adapter card, or Packet Microwave Adapter card) or port or facility failures (SFP or cut fiber). If a loopback address is used, PTP packets may arrive on any router network interface and the PTP clock remains up.

The 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, and 7705 SAR-X support only one PTP timeReceiver clock. This timeReceiver clock can be configured as the source of reference (ref1 or ref2) to the SSU.

6.4.7.13 PTP Ethernet capabilities

The 7705 SAR can be configured to transmit and receive PTP messages over a port that uses Ethernet encapsulation. The encapsulation type can be null, dot1q, or qinq. Ethernet-encapsulated PTP messages are processed on the node CSM or CSM functional block, and they are supported on ordinary timeReceiver, ordinary timeTransmitter, or boundary clocks for either frequency or time of day/phase recovery. The 7705 SAR-Ax can also support a grandmaster clock. The 7705 SAR-H, 7705 SAR-Wx, 7705 SAR-8 Shelf V2, and 7705 SAR-18 can also support a grandmaster clock when equipped to support GNSS. A PTP clock using Ethernet encapsulation can support up to 50 external peer clocks.

All platforms and cards that support PTP functionality support Ethernet-encapsulated PTP messages, except for the 2-port 10GigE (Ethernet) Adapter card/module . See Table 25: IEEE 1588v2 PTP support per fixed platform and Table 26: IEEE 1588v2 PTP support per card on the 7705 SAR-8 Shelf V2 and 7705 SAR-18 for a complete list of supported platforms and cards.

Ethernet encapsulation is configured on a per-port basis using the **config>system> ptp>clock** command, with the *clock-id* parameter set to **csm**. Ports can simultaneously support IPv4-encapsulated or IPv6-encapsulated PTP messages and Ethernet-encapsulated PTP messages. As well, the 7705 SAR supports the interworking of a PTP timeReceiver using IPv4-encapsulated or IPv6-encapsulated messages with a PTP timeTransmitter using Ethernet-encapsulated messages.

When a PTP clock is configured for Ethernet encapsulation, the following profiles are available:

- **ieee1588-2008**
- **g8275dot1-2014**
- **iec-61850-9-3-2016**
- **c37dot238-2017**

The following table describes the supported message rates for timeReceiver and timeTransmitter states for Ethernet-encapsulated PTP traffic, based on the profile configured. The ordinary clock can be either in the timeReceiver or timeTransmitter state. The boundary clock can be in both of these states.

Table 30: Rates for Ethernet-encapsulated PTP messages

Message/rate		ieee1588-2008	g8275dot1-2014	iec-61850-9-3-2016 c37dot238-2017
Announce	Minimum rate	1 per 16 seconds	1 per 16 seconds	1 per 16 seconds
	Maximum rate	8 per second	8 per second	8 per second
	Default rate	1 per 2 seconds	8 per second	1 per second
Sync	Minimum rate	1 per second	1 per second	1 per second
	Maximum rate	64 per second	64 per second	64 per second
	Default rate	64 per second	16 per second	1 per second
Delay	Minimum rate	1 per second	1 per second	1 per second
	Maximum rate	64 per second	64 per second	64 per second
	Default rate	64 per second	16 per second	1 per second

See Table 27: Rates for IP-encapsulated PTP messages for the supported message rates for IP-encapsulated PTP traffic.

PTP messages are transported within Ethernet frames with the Ethertype set to 0X88F7. Ports can be configured with one of two reserved multicast destination addresses:

- 01-1B-19-00-00-00 — used for all PTP messages except for peer delay mechanism messages
- 01-80-C2-00-00-0E — used for peer delay mechanism messages

Either address can be used for all messages depending on customer requirements. See Recommendation ITU-T G.8275.1/Y.1369.1. When the profile configuration is **iec-61850-9-3-2016** or **c37dot238-2017**, the 01-80-C2-00-00-0E address must be used for peer delay. See IEC/IEEE 61850-9-3 and the C37.238-2017 extension.

When the profile configuration is **ieee1588-2008**, **iec-61850-9-3-2016**, or **c37dot238-2017**, the PTP clock's priority1 and priority2 settings are used by the BTCA to help determine which clock should provide timing for the network. When the profile configuration is **g8275dot1-2014**, the **local-priority** value is used to choose between PTP timeTransmitters in the BTCA.

6.4.7.14 ITU-T G.8275.1 and G.8275.2

The 7705 SAR supports Recommendation ITU-T G.8275.1 and Recommendation ITU-T G.8275.2, which specify the architecture that allows the distribution of time and phasing. ITU-T G.8275.1 supports full timing support from the network and ITU G.8275.2 supports partial timing support (PTS) and assisted partial timing support (APTS). If a PTP clock is configured for G.8275.2 without GNSS, it uses PTS; if it is configured for GNSS, it can use APTS. It is assumed that these profiles will be used in well-planned cases where network behavior and performance can be constrained within well-defined limits, including limits on static asymmetry. When configured for the G.8275.1 or G.8275.2 profile, the 7705 SAR can operate as a boundary clock, an ordinary timeTransmitter clock, or an ordinary timeReceiver clock.

When the 7705 SAR is configured for the G.8275.1 or G.8275.2 profile, it uses an alternate BTCA for best timeTransmitter clock selection. This BTCA includes a PTP dataset comparison that is defined in IEEE 1588-2008, but with the following differences:

*   the **priority1** attribute value is removed from the dataset comparison
*   the **master-only** parameter value must be considered
*   multiple active grandmaster clocks are allowed; therefore, the BTCA will select the nearest clock of equal quality
*   a port-level **local-priority** attribute value is used to select a timeReceiver port if two ports receive an Announce message. This attribute is used as a tiebreaker in the dataset comparison algorithm if all other previous attributes of the datasets being compared are equal.
*   the **local-priority** parameter value is considered for the default dataset

The ITU-T G.8275.1 and G.8275.2 profiles have the following characteristics:

*   The default domain setting is 24 for G.8275.1; the allowed range is 0 to 255.

    The default domain setting is 44 for G.8275.2; the allowed range is 0 to 255.

*   Both one-step and two-step clocks are supported on timeReceiver-capable PTP ports.
*   G.8275.2 supports IP encapsulation.

    G.8275.1 supports IP encapsulation and Ethernet encapsulation. When Ethernet encapsulation is used, the following points apply:

    – Ethernet multicast addressing is used for transmitting PTP messages. Both the non-forwardable multicast address 01-80-C2-00-00-0E and forwardable multicast address 01-1B-19-00-00-00 are supported.

    – Virtual local area network (VLAN) tags within Ethernet frames carrying PTP messages are not supported. When a PTP clock receives a PTP message within a frame containing a VLAN tag, it discards this frame. A PTP clock that is compliant with the profile described in Recommendation ITU-T G.8275.1 must comply with IEEE 1588 – 2008 Annex F.

*   Synchronization messages are sent at a rate of 16 packets/s; Announce messages are sent at a rate of 8 packets/s.
*   On the 7705 SAR, the priority1 value is set to the default value (128) and cannot be changed.
*   On the 7705 SAR, if the **clock-type** parameter is set to **ordinary slave**, the priority2 value is set to the default value (255) and cannot be changed.

For further details, see Recommendation ITU-T G.8275.1/Y.1369.1 and Recommendation ITU-T G.8275.2/Y.1369.2.

6.4.7.14.1 ITU-T G.8275.2 APTS with asymmetry compensation

The ITU-T G.8275.2 APTS functionality is supported on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18 when equipped with a GNSS Receiver card and two Ethernet adapter cards — one configured as a G.8275.2 timeReceiver clock for backup and one configured as a G.8275.2 boundary clock with timeTransmitter ports.

When the PTP clock is configured to use the G.8275.2 profile and the integrated GNSS is configured and operationally up, GNSS is the active reference for both time/phase and frequency for the system. For extra resilience, APTS can be deployed when the following conditions are met:

- a G.8275.2 timeReceiver clock (an IP PTP clock 1 to 8) is configured on an Ethernet adapter card for IP-encapsulated PTP and **apts-asymmetry-compensation** is enabled

- a G.8275.2 boundary clock (a different IP PTP clock 1 to 8) is configured on another Ethernet adapter card for IP-encapsulated PTP

- the synchronous equipment timing source (SETS) is configured for GNSS as the first preference using the **config>system>sync-if-timing>ref1** command, PTP is configured as the second preference using the **config>system>sync-if-timing>ref2** command, and the **config>system>sync-if-timing>ref-order** command is configured to set the timing priority; in addition, SETS must be configured for revertive switching using the **config>system>sync-if-timing>revert** command

- the time clock is configured with GNSS as the first preference and the PTP backup clock as the second preference

Even though GNSS is the active reference, the backup timeReceiver PTP port has an active session with an upstream PTP grandmaster clock through a non-PTP network.

When GNSS is up, the level of asymmetry on the designated backup timeReceiver clock is monitored when the **apts-asymmetry-compensation** command is enabled. The CSM notes the time and frequency recovery state and the delay asymmetry of the backup timeReceiver clock based on the timestamps exchanged during the last update. If GNSS fails, the measured level of asymmetry is applied to the PTP backup clock to keep time and phase as accurate as possible. The monitored states and values are available via the CLI and SNMP.

The following table is from Recommendation ITU-T G.8275.2/Y.1369.2 (11/2022). It describes the mapping between the ITU-T G.8275.2 and PTP clock types. T-BC-A and T-TSC-A clocks apply to APTS.

Table 31: Mapping between ITU-T G.8275.2 and PTP clock types

Clock type from ITU-T G.8275.2	Description	Clock type from IEEE 1588
T-GM	timeTransmitter ordinary clock (clock with a single PTP port; cannot be a timeReceiver from another PTP clock)	Ordinary clock
	timeTransmitter boundary clock (clock with multiple PTP ports; cannot be a timeReceiver from another PTP clock)	Boundary clock[1]
T-BC-P (partial)	Boundary clock (may become a grandmaster clock or may be a timeReceiver from another PTP clock)	Boundary clock
T-BC-A (assisted partial)	Boundary clock assisted by a local time reference that is used as a primary source of time (may become a grandmaster clock or may be a timeReceiver to another PTP clock)	Boundary clock[2]
T-TSC-P (partial)	Always timeReceiver; single-port ordinary clock	Ordinary clock

Clock type from ITU-T G.8275.2	Description	Clock type from IEEE 1588
	PTP clock at the end of the PTP synchronization chain; multiple port clock	Boundary clock[1]
T-TSC-A (assisted partial)	Always timeReceiver; single-port ordinary clock assisted by a local time reference that is used as a primary source of time	Ordinary clock[2]
	PTP clock at the end of the PTP synchronization chain; multiple-port clock assisted by a local time reference that is used as a primary source of time	Boundary clock[1, 2]

Notes:

1. According to IEEE 1588, a clock that has multiple PTP ports is by definition a boundary clock.

2. Examples of local time references are a PRTC or a GNSS-based time source.

6.4.7.14.1.1 GNSS failure and recovery with APTS

When the G.8275.2 profile is used for GNSS-enabled 7705 SAR platforms, the APTS function frequently measures and stores the delay offset between the GNSS time and a backup PTP session time.

If GNSS fails, the time and frequency reference automatically switches from GNSS to the backup PTP timeReceiver clock, and the stored delay offset value is added to or subtracted from the backup PTP session to keep time and phase for the router as accurate as possible. After switching to the backup PTP timeReceiver clock, the clockClass output from the boundary clock corresponds to the clockClass from the backup PTP parent clock. If the clockClass of the parent clock is 6, the clockClass output of the boundary clock is 6 throughout the time reference switch operation.

When GNSS recovers after a failure, the boundary clock time reference switches back to GNSS from the backup PTP timeReceiver clock. Assuming that the asymmetry from the backup PTP has remained constant, the time to switch to the downstream clocks is minimal.

The switch back to GNSS must wait until GNSS time recovery stabilization is complete. After switching back to GNSS, the output clockClass of the boundary clock should be 6. If the backup PTP parent clock was also 6, the clockClass output of the boundary clock is 6 throughout the time reference switch operation.

If a failure occurs and neither GNSS nor the PTP backup is available, the PTP boundary clock enters holdover. The clockClass output from the boundary clock is 165.

For information about the values for the clockClass, time traceable flag, and frequency traceable flag, see Table 3 in Recommendation ITU-T G.8275.2/Y.1369.2 (11/2022).

6.4.7.14.2 Synchronization certainty/uncertainty

As described in Best TimeTransmitter Clock Algorithm, timeTransmitter clocks transmit Announce messages containing the clock priority and quality. Each clock in the network can use the BTCA and the clock properties received from the Announce messages to select the best clock to synchronize to.

Within a PTP-aware network, there could be situations where boundary clocks advertise clockClass 6 in the Announce message, which indicates that the parent clock is connected to a traceable primary reference source/clock (PRS/PRC) in locked mode (for example, locked to GNSS), and is therefore designated as the synchronization time source. However, the PTP network may still be in a transient state and stabilizing.

For example, this may occur when:

- a grandmaster clock locks and relocks to GNSS
- an intermediate boundary clock is started or restarted
- a new parent clock is chosen

Depending on the application, it may be important for a downstream boundary clock or timeReceiver clock to know whether the PTP network has stabilized or is still "synchronization uncertain".

Specifically when the G.8275.1profile (with IP encapsulation) or the G.8275.2 profile is used, the synchronizationUncertain flag is added to the Announce message. The use of this flag is optional. The 7705 SAR PTP grandmaster, boundary, and timeReceiver clocks support the processing of the synchronization state as follows.

- If a grandmaster clock has its synchronous equipment timing source (SETS) frequency clock and time clock locked to GNSS and its clockClass equals 6, it is in a "synchronization certain" state. The synchronizationUncertain flag in the Announce message is set to FALSE.

- If a grandmaster clock does not meet the above criteria, it is in a "synchronization uncertain" state. The synchronizationUncertain flag in the Announce message is set to TRUE.

- In order for a boundary clock to be in the "synchronization certain" state, its parent clock's clockClass must be "synchronization certain", its SETS must be locked and PRS/PRC traceable, and PTP must have sufficient time to stabilize to the parent clock. At that point, its PTP port state transitions from an Uncalibrated state to a TimeReceiver state.

  The transition period is 16 s for G.8275.1 and 256 s for G.8275.2. To be selected as a system time reference, a G.8275.1 or G.8275.2 clock must be in the "synchronization certain" state.

- A boundary clock can fall back to the "synchronization uncertain" state if its parent clock changes to the "synchronization uncertain" state, its SETS becomes unlocked or not PRS/PRC traceable, or the local clock is restarted or reset. The PTP port state transitions away from the TimeReceiver state.

This behavior is shown in the following figure.

Figure 22: Synchronization certain/uncertain states
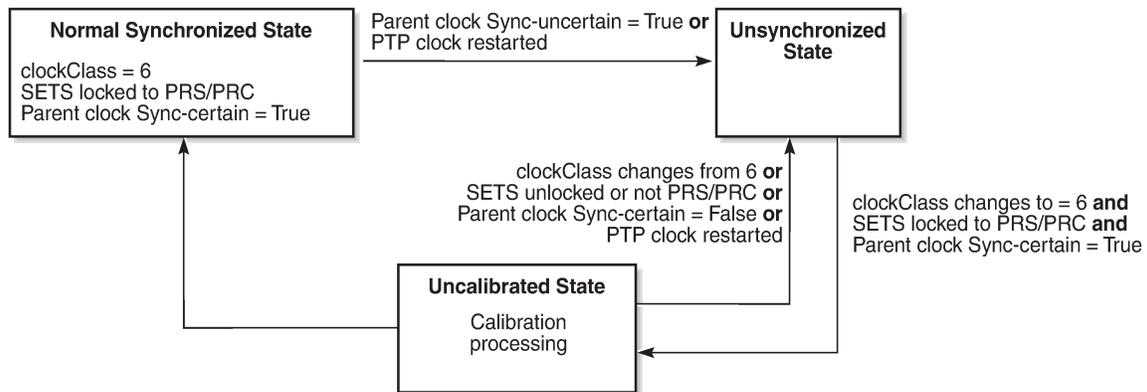
Because the synchronizationUncertain flag is newly agreed upon in standards, most base station timeReceiver clocks do not look at this bit. Therefore, in order to ensure that the downstream clocks are aware of the state of the network, the PTP clock (grandmaster, boundary, timeReceiver) may optionally be configured to transmit Announce and Sync messages only if the clock is in a "synchronization certain" state. This is done using the **no tx-while-sync-uncertain** command.

6.4.7.15 IEC/IEEE 61850-9-3 and C37.238-2017

The 7705 SAR supports IEC/IEEE 61850-9-3 and the C37.238-2017 extension, which are profiles that allow PTP to act as a timing source in power utility networks.

The IEC/IEEE 61850-9-3 and C37.238-2017 profiles support only Ethernet encapsulation with multicast addressing. Both profiles use the peer delay mechanism instead of the delay-request/response mechanism.

When configured for IEC/IEEE 61850-9-3 or C37.238-2017, the 7705 SAR can operate as a grandmaster clock, a boundary clock, or an ordinary timeReceiver clock and supports recovery of frequency as well as time of day/phase. Grandmaster clock functionality is only available for 7705 SAR variants with integrated GNSS.

Synchronous Ethernet can be used for frequency recovery as an optional mode for best time/phase recovery.

The IEC/IEEE 61850-9-3 and C37.238-2017 profiles have the following characteristics.

- The default domain setting is 0 for IEC/IEEE 61850-9-3 and 254 for C37.238-2017; the allowed range is 0 to 255.

- One-step clock operation is supported, without the need for follow-up messages.

- When Ethernet encapsulation is used, virtual local area network (VLAN) tags within Ethernet frames carrying PTP messages are not supported. When a PTP clock receives a PTP message within a frame containing a VLAN tag, it discards this frame.

- Synchronization messages, Announce messages, and peer delay messages are sent, by default, at the rate of 1 packet/s.

- By default, the priority1 and priority2 values are set to 255 when the clock type is ordinary timeReceiver and 128 when the clock type is ordinary timeTransmitter. The priority values can be configured to be between 0 and 255.

The C37.238-2017 profile uses the IEEE_C37_238 TLV in Announce messages between the parent and timeReceiver clocks. This TLV includes the grandmaster clock ID and the total time inaccuracy. Each clock in the chain adds its own inaccuracy to the total time inaccuracy, which gives the ultimate timeReceiver clock an estimate of the inaccuracy over the entire path.

The grandmaster inaccuracy includes the source time inaccuracy and the grandmaster time inaccuracy. When acting as a boundary clock, the system receives the total time inaccuracy from the parent clock and adds its own time inaccuracy, then sends out a TLV with the updated total time inaccuracy. By default, the time inaccuracy value is 100 ns for a grandmaster clock and 50 ns for a boundary clock. The default value can be changed for a boundary clock with the **time-inaccuracy-override** command.

For further details, see the IEC/IEEE 61850-9-3 standard and the C37.238-2017 extension.

6.4.7.16 PTP profile interworking

The PTP profile interworking feature allows the 7705 SAR to interwork a primary PTP profile with ports using alternate profiles connected to external devices. The 7705 SAR supports single-clock and multi-clock PTP profile interworking.

6.4.7.16.1 Single-clock PTP profile interworking

Single-clock PTP profile interworking allows the 7705 SAR to use G.8275.1 as a primary PTP profile while interworking with ports using alternate profiles connected to external devices. The profiles must support Ethernet encapsulation. The 7705 SAR supports one primary profile for interworking, which must be configured as G.8275.1, and up to two alternate profiles, which can be configured as either IEC/IEEE 61850-9-3 or C37.238-2017.

By default, all PTP ports use the primary profile. The port must be shut down before the profile configuration can be modified. Any port that uses an alternate profile must be shut down before the alternate profile configuration can be modified.

Only messages exchanged on interfaces using the primary profile are included in the BTCA for the PTP clock. Interfaces using an alternate profile are considered to have their **master-only** value set to **true** and ignore any Announce messages they receive.

The PTP clock follows the BTCA rules of the primary profile and updates all datasets appropriately. Interfaces using an alternate profile use the datasets of the PTP clock to populate fields in PTP messages. However, some values from the primary profile are modified because they are incompatible with values expected by the alternate profiles. The message rates used for the Announce messages may differ between profiles. The Announce rate is controlled by the **log-anno-interval** command configured for the profile in use. The Sync and Delay message rates are controlled by the per-port configuration.

The clockClass value in the Announce message may need to be converted (as shown in the following table) when interworking from a G.8275.1 primary profile to either the IEC/IEEE 61850-9-3 or C37.238-2017 alternate profile.

Table 32: ClockClass conversion for PTP interworking

From primary profile	To alternate profile
6	6 [1]
7	7
All other values	187

Note:

1. For normal-locked, time-traceable, and frequency-traceable

See IEC/IEEE 61850-9-3 and C37.238-2017 for more information about these profiles.

6.4.7.16.2 Multi-clock PTP profile interworking

Multi-clock PTP profile interworking allows the 7705 SAR to interwork multiple PTP profile combinations with a mix of IP and Ethernet encapsulations. With multi-clock PTP profile interworking, there are two active PTP clocks in the system: one PTP clock with Ethernet encapsulation (*clock-id* parameter set to **csm**) and one PTP clock with IP encapsulation (*clock-id* parameter set to 1 to 12). Multi-clock interworking is supported on the 7705 SAR-8 and 7705 SAR-18 on 8-port Gigabit Ethernet Adapter cards and 6-port Ethernet 10Gbps Adapter cards.

To assign a clock profile to be the primary clock, configure the system time to recover time from its clock ID with the **config>system>time>ptp>clock** command. To assign a clock profile to be the alternate clock, enable the **use-node-time** command on its clock ID. The alternate clock uses the timing reference recovered from the primary profile clock.

If the Ethernet encapsulated clock is the primary clock (the main router clock), the IP encapsulated clock must be the alternate clock that uses the primary clock as reference. The reverse is true if the IP encapsulated clock is the primary clock.

If the node time clock is based on the integrated GNSS, both PTP clocks can be timeTransmitter clocks for their respective profiles. In this scenario, there is no profile interworking because there is no way to determine which clock is the primary clock and which is the alternate clock.

The primary clock can be a timeTransmitter, boundary, or timeReceiver. The alternate clock must be configured to be a timeTransmitter for multi-clock PTP profile interworking.

The supported profile combinations are:

- primary profile is G.8275.2 (IP encapsulation) and alternate profile is G.8275.1 (Ethernet encapsulation)
- primary profile is G.8275.2 (IP encapsulation) and alternate profile is IEC/IEEE 61850-9-3 (Ethernet encapsulation)
- primary profile is G.8275.2 (IP encapsulation) and alternate profile is C37.238-2017 (Ethernet encapsulation)
- primary profile is G.8275.1 (Ethernet encapsulation) and alternate profile is G.8275.2 (IP encapsulation)

The frequency reference used by the alternate PTP clock is based on the SETS configuration which can be the integrated GNSS, PTP, or any other acceptable frequency reference available on the 7705 SAR. G.8275.1 PTP is not a valid reference for frequency.

6.4.7.17 PTP statistics

The 7705 SAR provides the capability to collect statistics, state, and events data for the PTP timeReceiver clock's interaction with PTP peer clock 1 and PTP peer clock 2. This data is collected separately for each peer clock and can be displayed using the **show system ptp clock ptp-port** command. This data can be used to monitor the PTP timeReceiver clock performance in relation to the peer clocks and to diagnose a problem or analyze the performance of a packet switched network for the transport of synchronization messages. The following data is collected:

PTP peer-1/PTP peer-2 statistics:

- number of signaling packets
- number of unicast request announce packets
- number of unicast request announce timeouts
- number of unicast request announce packets rejected
- number of unicast request synchronization packets
- number of unicast request synchronization timeouts
- number of unicast request synchronization packets rejected
- number of unicast request delay response packets
- number of unicast request delay response packets timeouts
- number of unicast request delay response packets rejected
- number of unicast grant announce packets
- number of unicast grant announce packets rejected
- number of unicast grant synchronization packets
- number of unicast grant synchronization packets rejected
- number of unicast grant delay response packets
- number of unicast grant delay response packets rejected
- number of unicast cancel announce packets
- number of unicast cancel synchronization packets
- number of unicast cancel delay response packets
- number of unicast acknowledge cancel announce packets
- number of unicast acknowledge cancel synchronization packets
- number of unicast acknowledge cancel delay response packets
- number of announce packets
- number of synchronization packets
- number of follow-up packets
- number of delay response packets
- number of delay request packets
- number of out-of-order synchronization packets
- total number of UDP (port 320) packets

- total number of UDP (port 319) packets

- number of alternate timeTransmitter packets discarded

- number of bad domain packets discarded

- number of bad version packets discarded

- number of duplicate messages packets discarded

- number of step RM greater than 255 discarded

PTP timeTransmitter-1/PTP timeTransmitter-2 algorithm state statistics (in seconds):

- number of free-run states

- number of acquiring states

- number of phase-tracking states

- number of hold-over states

- number of locked states

PTP timeTransmitter-1/PTP timeTransmitter-2 algorithm event statistics:

- number of excessive frequency errors detected

- number of excessive packet losses detected

- number of packet losses spotted

- number of excessive phase shifts detected

- number of high PDVs detected

- number of synchronization packet gaps detected

6.4.8 Synchronous Ethernet

Synchronous Ethernet is a variant of line timing that derives the physical layer transmitter clock from a high-quality timing reference, traceable to a primary reference clock. Synchronous Ethernet uses the physical layer of the Ethernet link to distribute a common clock signal to all nodes in the network. Each node has a local or system clock that determines the outgoing clock rate of each interface. The system clock of each node in the network is derived from the incoming clock at an input interface or from a dedicated timing interface; for example, a BITS port.

Synchronous Ethernet works at Layer 1 and is concerned only with the precision of the timing of signal transitions to relay and recover accurate frequencies. It is not impacted by traffic load and is therefore not affected by packet loss or PDV that occurs with timing methods that use higher layers of the networking technology.

Synchronous Ethernet is automatically enabled on ports and SFPs that support synchronous Ethernet. The operator can select an Ethernet SFP port as a candidate timing reference. The recovered timing from this port is distributed to the nodes in the network over the physical layer of the Ethernet link. This allows the operator to ensure that any of the system outputs are locked to a stable, traceable frequency source. The transmit timing of all SFP ports with SFPs that support synchronous Ethernet is then derived from the node's SSU.

Synchronous Ethernet can only be used for end-to-end network synchronization when all intermediate switching nodes in the network have hardware and software support for synchronous Ethernet.

Synchronous Ethernet is supported on the following cards and platforms:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card
- 2-port 10GigE (Ethernet) Adapter card
- 2-port 10GigE (Ethernet) module
- 10-port 1GigE/1-port 10GigE X-Adapter card
- Packet Microwave Adapter card
- 6-port SAR-M Ethernet module
- 7705 SAR-M (on all Ethernet ports)
- 7705 SAR-Hc (on all Ethernet ports)
- 7705 SAR-Wx (on all Ethernet ports)
- 7705 SAR-H (on all Ethernet ports)
- 7705 SAR-A (supported on the XOR ports (1 to 4), configured as either RJ45 ports or SFP ports, and on SFP ports 5 to 8. Ports 9 to 12 do not support synchronous Ethernet.)
- 7705 SAR-Ax (on all Ethernet ports)
- 7705 SAR-X (on all Ethernet ports)

If an SFP that does not support synchronous Ethernet is installed, the Ethernet card uses its local oscillator for transmit timing and an event is logged. If the Ethernet port is configured as a source of node synchronization and an SFP that does not support synchronous Ethernet is installed, a clock is not supplied to the SSU and an event is logged.

Each synchronous Ethernet port can be configured to recover received timing and send it to the SSU. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-Wx, any synchronous Ethernet-capable port can be used as an available reference. In addition, two references are available on the 7705 SAR-X and on the 2-port 10GigE (Ethernet) module or 6-port SAR-M Ethernet module. On the 7705 SAR-8 Shelf V2 and 7705 SAR-18, two references are available on:

- the 6-port Ethernet 10Gbps Adapter card
- the 8-port Gigabit Ethernet Adapter card
- the 2-port 10GigE (Ethernet) Adapter card
- the 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)
- the Packet Microwave Adapter card

Synchronous Ethernet ports always use node timing from the SSU. Configuration of one port automatically configures the other port.

If timing is recovered from a synchronous Ethernet port from an upstream non-synchronous Ethernet free-running port and selected as the reference to the SSU, then this clock may not be of sufficient quality or accuracy for node operations. This reference may be disqualified because the frequency may not be within the pull-in range of the SSU Stratum 3 oscillator.

On the 7705 SAR-M, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, 7705 SAR-X, and on the Packet Microwave Adapter card, a copper-based, RJ45 synchronous Ethernet port **phy-tx-clock** must be configured as **slave** before the port is configured to be a timing source for the node. If a copper-based, RJ45 synchronous Ethernet port is a timing source for the node, the port **phy-tx-clock** cannot be changed to another mode.

6.4.9 Synchronization Status Messaging with quality level selection

Synchronization Status Messaging (SSM) provides a mechanism for downstream network elements to determine the quality level of the source.

The quality level values are processed by the 7705 SAR system timing module (SSU) to track the network timing flow and select the highest-quality source. The selection process is described in Timing reference selection based on quality level. Also see Figure 23: Timing reference selection based on quality level. SSM also allows the network elements to autonomously reconfigure the timing path to select the best possible source for timing and to avoid timing loops. This function is especially useful in a ring topology where network timing may be passed in both directions around the ring.

Synchronization status messages containing the quality level values are placed in prescribed overhead bytes for SONET and SDH signals and in bit-oriented messages within the data link for DS1 (ESF) and E1 physical ports.

For synchronous Ethernet interfaces, there is no equivalent fixed location to convey synchronization status messages; therefore, the quality level values are transported using Ethernet frames over a message channel. This channel, called the Ethernet Synchronization Message Channel (ESMC), uses an Ethernet protocol based on an IEEE Organization Specific Slow Protocol (OSSP). The 4-bit quality level value is carried within a Type-Length-Value (TLV) byte of an Ethernet OAM Protocol Data Unit (PDU) that uses the OSSP subtype.

The clock source quality levels identified for the purpose of tracking network timing flow are listed below. They make up all of the defined network deployment options given in Recommendations G.803 and G.781 (option I pertains to the SDH model and Option II pertains to the SONET model).

The received quality level values for the two network options based on the specific interfaces within these options are provided in the first two columns of Table 33: Quality level (QL) values by interface type (SDH, SONET, SyncE) (for SONET, SDH, and Synchronous Ethernet interfaces) and Table 34: Quality level (QL) values by interface type (E1 and T1) (for E1 and T1 interfaces). The transmitted quality level values are shown in the last two columns of Table 33: Quality level (QL) values by interface type (SDH, SONET, SyncE) and Table 34: Quality level (QL) values by interface type (E1 and T1).

- prs — SONET Primary Reference Source Traceable
- stu — SONET Synchronous Traceability Unknown
- st2 — SONET Stratum 2 Traceable
- tnc — SONET Transit Node Clock Traceable
- st3e — SONET Stratum 3E Traceable
- st3 — SONET Stratum 3 Traceable
- smc — SONET Minimum Clock Traceable
- eec1 — SDH Ethernet Equipment Clock Option 1 Traceable
- eec2 — SONET Ethernet Equipment Clock Option 2 Traceable
- prc — SDH Primary Reference Clock Traceable
- ssu-a — SDH Primary Level Synchronization Supply Unit Traceable
- ssu-b — SDH Second Level Synchronization Supply Unit Traceable
- sec — SDH Synchronous Equipment Clock Traceable

The user may override the received quality level value of the system synchronization reference input by using the **ql-override** command to configure one of the above values as a static value. This in turn may affect the transmitted quality level value on each SSM-capable port. Also, the user may use the **tx-dus**

command to force the quality level value that is transmitted on the SSM channel to be set to dnu (do not use) or dus (do not use for synchronization). This capability is provided to block the interface from being a timing source for the 7705 SAR. The dus/dnu quality level value cannot be overridden.

Figure 23: Timing reference selection based on quality level
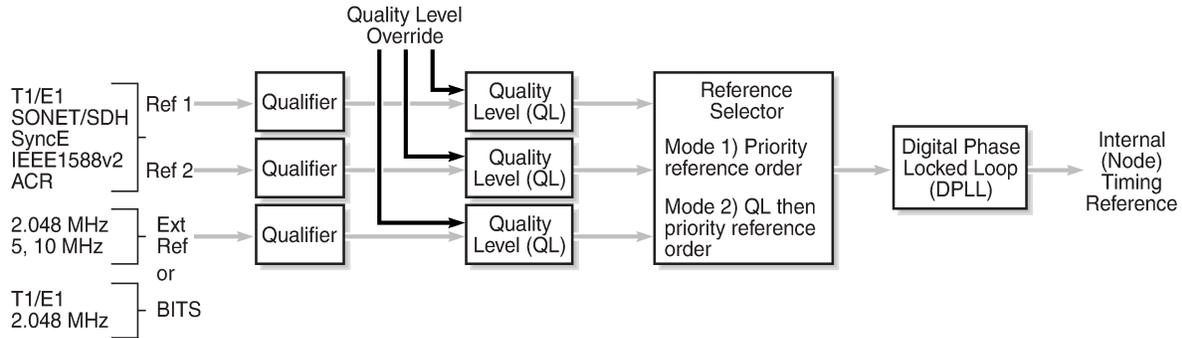
20935

The G.803 and G.781 standards also define additional codes for internal use.

- QL-INVx is generated internally by the system when an unallocated synchronization status message value is received; x represents the binary value of this synchronization status message. Within the 7705 SAR, all these independent values are assigned a single value of QL-INVALID.

- QL-FAILED is generated internally by the system when the terminated network synchronization distribution trail is in the signal fail state.

- QL-UNKNOWN is generated internally by the system to differentiate from a received QL-STU code. It is equivalent to QL-STU for the purposes of quality level selection.

- If the node clock is in a holdover state, a holdover message is generated internally by the system and the transmitted SSM quality level value on an SSM-capable port is st3, eec1, eec2, or ssu-b, depending on the type of interface (as shown in Table 33: Quality level (QL) values by interface type (SDH, SONET, SyncE) and Table 34: Quality level (QL) values by interface type (E1 and T1)).

Table 33: Quality level (QL) values by interface type (SDH, SONET, SyncE)

SSM quality level value received on port		Internal relative quality level	SSM quality level value to be transmitted	
SDH interface SyncE interface in SDH mode	SONET interface SyncE interface in SONET mode		SDH interface SyncE interface in SDH mode	SONET interface SyncE interface in SONET mode
0010 (prc)	0001 (prs)	Best quality [1]	0010 (prc)	0001 (prs)
—	0000 (stu)		0100 (ssu-a)	0000 (stu)
—	0111 (st2)		0100 (ssu-a)	0111 (st2)
0100 (ssu-a)	0100 (tnc)		0100 (ssu-a)	0100 (tnc)
—	1101 (st3e)		1000 (ssu-b)	1101 (st3e)

SSM quality level value received on port		Internal relative quality level	SSM quality level value to be transmitted	
SDH interface **SyncE interface in SDH mode**	**SONET interface** **SyncE interface in SONET mode**		**SDH interface** **SyncE interface in SDH mode**	**SONET interface** **SyncE interface in SONET mode**
1000 (ssu-b)	—		1000 (ssu-b)	1010 (st3/eec2)
—	1010 (st3/eec2)		1011 (sec/eec1)	1010 (st3/eec2)
1011 (sec/eec1)	—	Lowest quality qualified in QL-enabled mode	1011 (sec/eec1)	1100 (smc)
—	1100 (smc)	See note [2]	1111 (dnu)	1100 (smc)
1111 (dnu)	1111 (dus)	See note [2]	1111 (dnu)	1111 (dus)
Any other	Any other	QL-INVALID	1111 (dnu)	1111 (dus)
—	—	QL-FAILED	1111 (dnu)	1111 (dus)
—	—	QL-UNC	1011 (sec/eec1)	1010 (st3/eec2)

Notes:

1. As the received QL on the port drops from prc/prs to sec/eec1 (row 1 to row 8), the quality level of the internal SSU drops from "Best quality" to "Lowest quality".

2. These quality level indications are considered to be lower than the internal clock of the system. They are relayed to the line interfaces when ql-selection is disabled. When ql-selection is enabled, these inputs are never selected. If there is no valid reference available for the internal clock, then the clock enters holdover mode and the quality level is QL-UNC.

Table 34: Quality level (QL) values by interface type (E1 and T1)

SSM quality level value received on port		Internal relative quality level	SSM quality level value to be transmitted	
E1 interface	**T1 interface (ESF)**		**E1 interface**	**T1 interface (ESF)**
0010 (prc)	00000100 11111111 (prs)	Best quality[1]	0010 (prc)	00000100 11111111 (prs)
—	00001000 11111111 (stu)		0100 (ssu-a)	00001000 11111111 (stu)
—	00001100 11111111 (st2)		0100 (ssu-a)	00001100 11111111 (st2)
0100 (ssu-a)	01111000 11111111 (tnc)		0100 (ssu-a)	01111000 11111111 (tnc)

SSM quality level value received on port		Internal relative quality level	SSM quality level value to be transmitted	
E1 interface	T1 interface (ESF)		E1 interface	T1 interface (ESF)
—	01111100 11111111 (st3e)		1000 (ssu-b)	01111100 11111111 (st3e)
1000 (ssu-b)	—		1000 (ssu-b)	00010000 11111111 (st3)
—	00010000 11111111 (st3)		1011 (sec)	00010000 11111111 (st3)
1011 (sec)	—	Lowest quality qualified in QL-enabled mode	1011 (sec)	00100010 11111111 (smc)
—	00100010 11111111 (smc)	See note [2]	1111 (dnu)	00100010 11111111 (smc)
1111 (dnu)	00110000 11111111 (dus)	See note [2]	1111 (dnu)	00110000 11111111 (dus)
Any other	N/A	QL-INVALID	1111 (dnu)	00110000 11111111 (dus)
—	—	QL-FAILED	1111 (dnu)	00110000 11111111 (dus)
—	—	QL-UNC	1011 (sec)	00010000 11111111 (st3)

Notes:

1. As the received QL on the port drops from prc/prs to sec/eec1 (row 1 to row 8), the quality level of the internal SSU drops from "Best quality" to "Lowest quality".

2. These quality level indications are considered to be lower than the internal clock of the system. They are relayed to the line interfaces when ql-selection is disabled. When ql-selection is enabled, these inputs are never selected. If there is no valid reference available for the internal clock, then the clock enters holdover mode and the quality level is QL-UNC.

6.4.9.1 Timing reference selection based on quality level

For a SONET/SDH interface, a BITS DS1 or E1 physical port, a DS1 or E1 port interface that supports SSM, or a synchronous Ethernet interface that supports ESMC, a timing input provides a quality level value to indicate the source of timing of the far-end transmitter. These values provide input to the selection processes on the nodal timing subsystem. This selection process determines which input to use to generate the signal on the SSM egress ports and the reference to use to synchronize the nodal clock, as described below.

- For the two reference inputs (ref1 and ref2) and for the BITS input ports, if the interface configuration supports the reception of a QL over SSM or ESMC, then the quality level value is associated with the timing derived from that input.

- For the two reference inputs and for the BITS input ports, if the interface configuration is T1 with SF framing, then the quality level associated with the input is QL-UNKNOWN.

- For the two reference inputs, if they are synchronous Ethernet ports and the ESMC is disabled, then the quality level value associated with that input is QL-UNKNOWN.

- For the two reference inputs and for the BITS input ports, if the interface configuration supports the reception of a QL over SSM (and not ESMC), and no SSM value has been received, then the quality level value associated with the input is QL-STU.

- For the two reference inputs and for the BITS input ports, if the interface configuration supports the reception of a QL over SSM or ESMC, but the quality level value received over the interface is not valid for the type of interface, then the quality level value associated with that input is QL-INVALID.

- For the two reference inputs, if they are external synchronization, DS3, or E3 ports, then the quality level value associated with the input is QL-UNKNOWN.

- For the two reference inputs, if they are synchronous Ethernet ports and the ESMC is enabled but no valid ESMC Information PDU has been received within the previous 5 s, then the quality level value associated with that input is QL-FAILED.

- If the user has configured an override for the quality level associated with an input, the node displays both the received and override quality level value for the input. If no value has been received, then the associated value is displayed instead.

After the quality level values have been associated with the system timing inputs, the two reference inputs and the external input timing ports are processed by the system timing module to select a source for the SSU. This selection process is described below.

- Before an input can be used as a potential timing source, it must be enabled using the **ql-selection** command. If **ql-selection** is disabled, then the priority order of the inputs for the Synchronous Equipment Timing Generator (SETG) is the priority order configured under the **ref-order** command.

- If **ql-selection** is enabled, then the priority of the inputs is calculated using the associated quality level value of the input and the priority order configured under the **ref-order** command. The inputs are ordered by the internal relative quality level (shown in the middle row in Table 33: Quality level (QL) values by interface type (SDH, SONET, SyncE)) based on their associated quality level values. If two or more inputs have the same quality level value, then they are placed in order based on where they appear in the **ref-order** priority. The priority order for the SETG is based on both the reference inputs and the external synchronization input ports.

- When a prioritized list of inputs is calculated, the SETG and the external synchronization output ports are configured to use the inputs in their respective orders.

- When the SETG and external synchronization output ports priority lists are programmed, then the highest-qualified priority input is used. To be qualified, the signal is monitored to ensure that it has the expected format and that its frequency is within the pull-in range of the SETG.

6.4.9.1.1 SSM/ESMC QL transmission

If a port is using the SETG output as its timing reference, the port transmits the SSM corresponding to the QL of the SETG.

On the port that is selected as the reference for the SETG, the port transmits the DNU/DUS value in the SSM/ESMC.

If a BITS port is selected as the reference for the SETG, both BITS ports transmit DNU/DUS value.

An Ethernet port with a copper SFP always transmits DNU/DUS when SSM is enabled on the port. When SSM is enabled on a copper-based RJ45 Ethernet port, DNU/DUS is transmitted if the port **phy-tx-clock** is not configured as **master**. When SSM is enabled on a copper-based RJ45 Ethernet port and the port **phy-tx-clock** is configured as **master**, the port transmits the SSM value corresponding to the determined by the SSU.

6.4.9.1.1.1 DS1 physical port QL transmission

DS1 signals can carry the quality level value of the timing source via the SSM transported within the 1544 kb/s signal Extended Super Frame (ESF) Data Link (DL), as specified in Recommendation G.704.

The format of the ESF data link messages is 0xxx xxx0 1111 1111, with the rightmost bit transmitted first. The 6 bits denoted by xxx xxx contain the message; some of these messages are reserved for synchronization messaging. It takes 32 frames (4 ms) to transmit all 16 bits of a complete DL message.

SSM over DS1 ESF is supported on the 7705 SAR-18 via the BITS ports and also on T1 ports on the 16-port T1/E1 ASAP Adapter card, the 32-port T1/E1 ASAP Adapter card, and the 7705 SAR-A, 7705 SAR-M, 7705 SAR-H, and 7705 SAR-X chassis.

6.4.9.1.1.2 E1 physical port QL transmission

E1 signals can carry the quality level value of the timing source via one of the Sa bits (Sa4 to Sa8) in a synchronization status message, as described in G.704, section 2.3.4. Choosing which Sa bit carries the SSM is user-configurable.

SSM over E1 is supported on the 7705 SAR-18 via the BITS ports. SSM via an E1 port is supported on the 16-port T1/E1 ASAP Adapter card, the 32-port T1/E1 ASAP Adapter card, and the 7705 SAR-A, 7705 SAR-M, and 7705 SAR-X chassis.

6.5 System configuration process overview

Figure 24: System Configuration and Implementation Flow displays the process to provision basic system parameters.

Figure 24: System Configuration and Implementation Flow
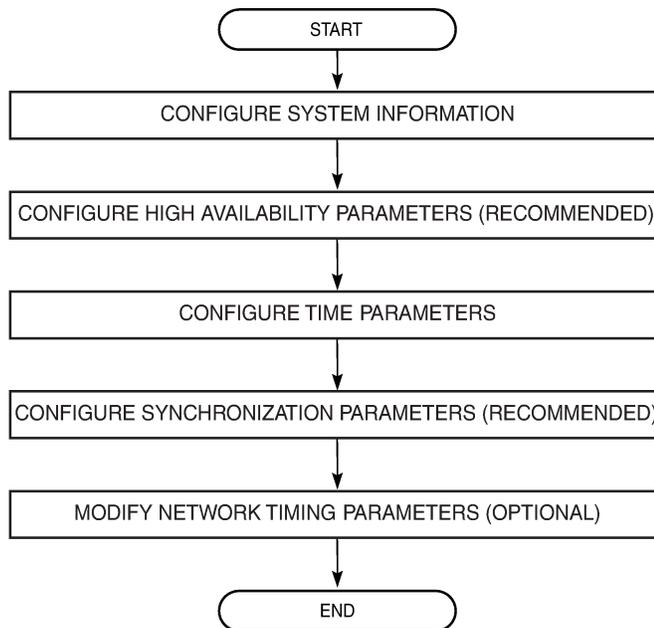
6.6 Configuration notes

This section describes system configuration guidelines and restrictions.

- The 7705 SAR must be properly initialized and the boot loader and BOF files successfully executed to access the CLI.

6.7 Configuring system management with CLI

This section provides information about configuring system management features with CLI.

Topics in this section include:

- System management configuration
- Basic system configuration
- Common configuration tasks
- Configuring system monitoring thresholds
- Configuring LLDP

6.8 System management configuration

6.8.1 Saving configurations

Whenever configuration changes are made, the modified configuration must be saved so that the changes are not lost when the system is rebooted. The system uses the configuration and image files, as well as other operational parameters necessary for system initialization, according to the locations specified in the boot options file (BOF). For more information about the BOF, see Boot options.

Configuration files are saved by executing explicit or implicit command syntax.

- An explicit save writes the configuration to the location specified in the **save** command syntax (the *file-url* option).

- An implicit save writes the configuration to the file specified in the primary configuration location.

  If the *file-url* option is not specified in the **save** command syntax, the system attempts to save the current configuration to the current BOF primary configuration source. If the primary configuration source (path and/or filename) changed since the last boot, the new configuration source is used.

The **save** command includes an option to save both default and non-default configuration parameters (the **detail** option).

The **index** option specifies that the system preserves system indexes when a **save** command is executed, regardless of the persistent status in the BOF file. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indexes are preserved between reboots, including the interface index, LSP IDs, and path IDs. This reduces resynchronizations of the Network Management System (NMS) with the affected network element.

If the save attempt fails at the destination, an error occurs and is logged. The system does not try to save the file to the secondary or tertiary configuration sources unless the path and filename are explicitly named with the **save** command.

6.9 Basic system configuration

This section provides information to configure system parameters and provides configuration examples of common configuration tasks. The minimal system parameters that should be configured are:

- System information parameters

- System time elements

The following example displays a basic system configuration:

```
ALU-1>config>system# info
#--------------------------------------
echo "System Configuration"
#--------------------------------------
        name "ALU-1"
        coordinates "Unknown"
        snmp
        exit
        security
            snmp
                community "private" rwa version both
            exit
```

```
            exit
            time
                ntp
                     server 192.168.15.221
                     no shutdown
                exit
                sntp
                     shutdown
                exit
                zone GMT
            exit
-------------------------------------------
ALU-1>config>system#
```

6.10 Common configuration tasks

This section provides a brief overview of the tasks that must be performed to configure system parameters and provides the CLI commands.

- System information
- Configuring script parameters
- Configuring synchronization and redundancy
- Configuring ATM parameters
- Configuring backup copies
- Configuring system administration parameters
- System timing

6.10.1 System information

This section covers the basic system information parameters to configure the physical location of the 7705 SAR, contact information, router location information such as an address, floor, and room number, global navigation satellite system (GNSS) coordinates, and system name.

Use the CLI syntax displayed below to configure the following system components:

- System information parameters
- System time elements

6.10.1.1 System information parameters

General system parameters include:

- Name
- Contact
- Location
- CLLI code
- Coordinates

- [System identifier](#)

6.10.1.1.1 Name

Use the **system name** command to configure a name for the device. The name is used in the prompt string. Only one system name can be configured. If multiple system names are configured, the last one encountered overwrites the previous entry.

Use the following CLI syntax to configure the system name:

CLI syntax:
```
config>system
    name system-name
```

Example:
```
config>system# name ALU-1
```

The following example displays the system name:

```
ALU-1>config>system# info
#----------------------------------------
echo "System Configuration"
#----------------------------------------
        name "ALU-1"
. . .
        exit
-----------------------------------------------
ALU-1>config>system#
```

6.10.1.1.2 Contact

Use the **contact** command to specify the name of a system administrator, IT staff member, or other administrative entity.

CLI syntax:
```
config>system
    contact contact-name
```

Example:
```
config>system# contact "Fred Information Technology"
```

6.10.1.1.3 Location

Use the **location** command to specify the system location of the device. For example, enter the city, building address, floor, and room number where the router is located.

Use the following CLI syntax to configure the location:

CLI syntax:
```
config>system
```

```
                         location location
```

Example:

```
config>system# location "Bldg.1-floor 2-Room 201"
```

6.10.1.1.4 CLLI code

The Common Language Location Code (CLLI code) is an 11-character standardized geographic identifier that is used to uniquely identify the geographic location of a 7705 SAR.

Use the following CLI command syntax to define the CLLI code:

CLI syntax:

```
config>system
    clli-code clli-code
```

Example:

```
config>system# clli-code abcdefg1234
```

6.10.1.1.5 Coordinates

Use the optional **coordinates** command to specify the GNSS location of the device. If the string contains spaces, the entire string must be enclosed within double quotes.

Use the following CLI syntax to configure the location:

CLI syntax:

```
config>system
    coordinates coordinates
```

Example:

```
config>system# coordinates "N 45 58 23, W 34 56 12"
```

The following example displays the configuration output of the general system commands:

```
ALU-1>config>system# info
#----------------------------------------
echo "System Configuration"
#----------------------------------------
name "ALU-1"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"

. . .
        exit
    -----------------------------------------
ALU-1>config>system#
```

6.10.1.1.6 System identifier

The system identifier is an IPv4 address that can be used to uniquely identify the 7705 SAR in the network in situations where the system IP address may change dynamically.

Use the following CLI command syntax to define the system identifier:

CLI syntax:
```
config>system
    identifier id
```

Example:
```
config>system# identifier 192.0.2.255
```

6.10.1.2 System time elements

The system clock maintains time according to Coordinated Universal Time (UTC). Configure information time zone and summer time (daylight savings time) parameters to correctly display time according to the local time zone.

Time elements include:

- Zone
- Summer time conditions
- NTP
- SNTP
- PTP
- Time-of-day measurement (ToD-1pps)
- GNSS
- CRON

Use the following CLI syntax to configure system time elements. The **authentication-key des** keyword is not supported if the 7705 SAR node is running in FIPS-140-2 mode.

CLI syntax:
```
config>system
time
    dst-zone zone-name
        end {end-week} {end-day} {end-month} [hours-minutes]
        offset offset
        start {start-week} {start-day} {start-month} [hours-minutes]
    gnss
        port port-id time-ref-priority priority-value
    ntp
        authentication-check
        authentication-key key-id {key key} [hash | hash2] {type des
| message-digest}
        broadcastclient [router router-name] {interface ip-int-name}
[authenticate]
        mda-timestamp
        multicastclient [authenticate]
        server {ip-address | ipv6-address} [key-id key-id]
[version version] [prefer]
        no shutdown
```

```
        ptp
            clock clock-id time-ref-priority priority-value
            clock csm time-ref-priority priority-value
        sntp
            broadcast-client
            server-address ip-address [version version-number] [normal |
 preferred] [interval seconds]
            no shutdown
        tod1-pps
            message-type {ct | cm | irig-b002-b122 | irig-b003-b123 | irig-
b006-b126 | irig-b007-b127}
        zone {std-zone-name | non-std-zone-name} [hh[:mm]]
```

6.10.1.2.1 Zone

The **zone** command sets the time zone and/or time zone offset for the router. The 7705 SAR supports system-defined and user-defined time zones. The system-defined time zones are listed in Table 35: System-defined time zones .

CLI syntax:

```
config>system>time
    zone {std-zone-name | non-std-zone-name} [hh [:mm]]
```

Example:

```
config>system>time# zone GMT
```

The following example displays the zone output:

```
ALU-1>config>system>time# info
----------------------------------------------
        ntp
                server 192.168.15.221
                no shutdown
        exit
        sntp
                shutdown
        exit
        zone UTC
----------------------------------------------
ALU-1>config>system>time#
```

Table 35: System-defined time zones

Acronym	Time zone name	UTC offset
Europe:		
GMT	Greenwich Mean Time	UTC
WET	Western Europe Time	UTC
WEST	Western Europe Summer Time	UTC +1 hour
CET	Central Europe Time	UTC +1 hour

Acronym	Time zone name	UTC offset
CEST	Central Europe Summer Time	UTC +2 hours
EET	Eastern Europe Time	UTC +2 hours
EEST	Eastern Europe Summer Time	UTC +3 hours
MSK	Moscow Time	UTC +3 hours
MSD	Moscow Summer Time	UTC +4 hours
US and Canada:		
AST	Atlantic Standard Time	UTC -4 hours
ADT	Atlantic Daylight Time	UTC -3 hours
EST	Eastern Standard Time	UTC -5 hours
EDT	Eastern Daylight Saving Time	UTC -4 hours
CST	Central Standard Time	UTC -6 hours
CDT	Central Daylight Saving Time	UTC -5 hours
MST	Mountain Standard Time	UTC -7 hours
MDT	Mountain Daylight Saving Time	UTC -6 hours
PST	Pacific Standard Time	UTC -8 hours
PDT	Pacific Daylight Saving Time	UTC -7 hours
HST	Hawaiian Standard Time	UTC -10 hours
AKST	Alaska Standard Time	UTC -9 hours
AKDT	Alaska Standard Daylight Saving Time	UTC -8 hours
Australia and New Zealand:		
AWST	Western Standard Time	UTC +8 hours
ACST	Central Standard Time	UTC +9.5 hours
AEST	Eastern Standard/Summer Time	UTC +10 hours
NZT	New Zealand Standard Time	UTC +12 hours
NZDT	New Zealand Daylight Saving Time	UTC +13 hours

6.10.1.2.2 Summer time conditions

The **dst-zone** command configures the start and end dates and offset for summer time or daylight savings time to override system defaults or for user-defined time zones.

When configured, the time is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.

CLI syntax:

```
config>system>time
    dst-zone zone-name
        end {end-week} {end-day} {end-month} [hours-minutes]
        offset offset
        start {start-week} {start-day} {start-month} [hours-minutes]
```

Example:

```
config>system>time# dst-zone pt
config>system>time>dst-zone# start second sunday april 02:00
end first sunday october 02:00
config>system>time>dst-zone# offset 0
```

If the time zone configured is listed in Table 35: System-defined time zones , then the starting and ending parameters and offset do not need to be configured with this command unless there is a need to override the system defaults. The command returns an error if the start and ending dates and times are not available either in Table 35: System-defined time zones or entered as optional parameters in this command.

The following example displays the configured parameters.

```
A:ALU-1>config>system>time>dst-zone# info
----------------------------------------------
            start second sunday april 02:00
            end first sunday october 02:00
            offset 0
----------------------------------------------
A:ALU-1>config>system>time>dst-zone# offset 0
```

6.10.1.2.3 NTP

Network Time Protocol (NTP) is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*. It allows for participating network nodes to keep time more accurately and maintain time in a synchronized manner between all participating network nodes.

NTP time elements include:

- Authentication-check
- Authentication-key
- Broadcastclient
- MDA-timestamp
- Multicastclient
- Server

CLI syntax:

```
config>system>time
```

```
        ntp
            authentication-check
            authentication-key key-id {key key} [hash | hash2] {type des |
    message-digest}
            broadcastclient [router router-name] {interface ip-int-name}
    [authenticate]
            mda-timestamp
            multicastclient [authenticate]
            server {ip-address | ipv6-address} [key-id key-id]
    [version version] [prefer]
            no shutdown
```

6.10.1.2.3.1 Authentication-check

The **authentication-check** command provides for the option to skip the rejection of NTP PDUs that do not match the authentication key or authentication type requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key ID, type, or key.

When authentication-check is configured, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for key ID, one for type, and one for key value mismatches.

CLI syntax:
```
config>system>time>ntp
    authentication-check
```

Example:
```
config>system>time>ntp# authentication-check
config>system>time>ntp# no shutdown
```

6.10.1.2.3.2 Authentication-key

This command configures an authentication key ID, key type, and key used to authenticate NTP PDUs sent to and received from other network elements participating in the NTP protocol. For authentication to work, the authentication key ID, authentication type, and authentication key value must match.

CLI syntax:
```
config>system>time>ntp
    authentication-key key-id {key key} [hash | hash2] type {des |
    message-digest}
```

Example:
```
config>system>time>ntp# authentication-key 1 key A type des
config>system>time>ntp# no shutdown
```

The following example shows NTP disabled with the **authentication-key** parameter enabled.

```
A:ALU-1>config>system>time>ntp# info
----------------------------------------------
            shutdown
            authentication-key 1 key "OAwgNUlbzgI" hash2 type des
----------------------------------------------
```

```
A:ALU-1>config>system>time>ntp#
```

6.10.1.2.3.3 Broadcastclient

The **broadcastclient** command enables listening to NTP broadcast messages on the specified interface.

CLI syntax:
```
config>system>time>ntp
    broadcastclient[router router-name] {interface ip-int-name}
 [authenticate]
```

Example:
```
config>system>time>ntp# broadcastclient interface int11
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the **broadcastclient** parameter enabled.

```
ALU-1>config>system>time# info
----------------------------------------------
         ntp
             broadcastclient interface int11
             no shutdown
         exit
         dst-zone PT
             start second sunday april 02:00
             end first sunday october 02:00
             offset 0
         exit
         zone UTC
----------------------------------------------
ALU-1>config>system>time#
```

6.10.1.2.3.4 MDA-timestamp

The **mda-timestamp** command enables timestamping on an adapter card by the network processor to allow more accurate timestamping for in-band NTP packets. Timestamping on an adapter card is only performed on Ethernet-based adapter cards. This command can only be set if NTP is shut down and all the NTP servers are not associated with an authentication key. This command does not change the behavior of NTP over the management port. Use the **no** form of this command to revert to the default behavior of having NTP packets timestamped by the CSM.

CLI syntax:
```
config>system>time>ntp
    mda-timestamp
```

Example:
```
config>system>time>ntp# mda-timestamp
config>system>time>ntp# no shutdown
```

The following example shows enhanced NTP performance enabled using the **mda-timestamp** command.

```
A:ALU-1>config>system>time>ntp# info
----------------------------------------------
```

```
                    shutdown
                    no authentication-key 1
                    mda-timestamp
        -----------------------------------------------
A:ALU-1>config>system>time>ntp#
```

6.10.1.2.3.5 Multicastclient

This command is used to configure an address to receive multicast NTP messages on the CSM Management port. The **no** form of this command removes the multicast client.

If multicastclient is not configured, all NTP multicast traffic is ignored.

CLI syntax:
```
config>system>time>ntp
    multicastclient [authenticate]
```

Example:
```
config>system>time>ntp# multicastclient authenticate
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the **multicastclient** command configured.

```
ALU-1>config>system>time# info
-----------------------------------------------
            server 192.168.15.221
            multicastclient
            no shutdown
-----------------------------------------------
ALU-1>config>system>time##
```

6.10.1.2.3.6 Server

The **server** command is used when the node should operate in client mode with the NTP server specified in the address field. Use the **no** form of this command to remove the server with the specified address from the configuration.

Up to five NTP servers can be configured.

CLI syntax:
```
config>system>time>ntp
    server {ip-address | ipv6-address} [key-id key-id] [version version]
 [prefer]
```

Example:
```
config>system>time>ntp# server 192.168.1.1 key-id 1
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the **server** command configured.

```
A:sim1>config>system>time>ntp# info
-----------------------------------------------
            no shutdown
            server 192.168.1.1 key 1
```

```
--------------------------------------------
A:sim1>config>system>time>ntp#
```

6.10.1.2.4 SNTP

SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from SNTP/NTP servers; it cannot be used to provide time services to other systems. SNTP can be configured in either broadcast or unicast client mode.

SNTP time elements include:

- Broadcast-client
- Server-address

CLI syntax:
```
config>system>time
    sntp
         broadcast-client
         server-address ip-address [version version-number] [normal |
 preferred] [interval seconds]
             no shutdown
```

6.10.1.2.4.1 Broadcast-client

The **broadcast-client** command enables listening at the global device level to SNTP broadcast messages on interfaces with broadcast client enabled.

CLI syntax:
```
config>system>time>sntp
    broadcast-client
```

Example:
```
config>system>time>sntp# broadcast-client
config>system>time>sntp# no shutdown
```

The following example shows SNTP enabled with the **broadcast-client** parameter enabled.

```
ALU-1>config>system>time# info
--------------------------------------------
        sntp
            broadcast-client
            no shutdown
        exit
        dst-zone PT
            start second sunday april 02:00
            end first sunday october 02:00
            offset 0
        exit
        zone GMT
--------------------------------------------
ALU-1>config>system>time#
```

6.10.1.2.4.2 Server-address

The **server-address** command configures an SNTP server for SNTP unicast client mode.

CLI syntax:
```
config>system>time>sntp
    server-address ip-address version version-number] [normal | preferred]
 [interval seconds]
```

Example:
```
config>system>time>sntp# server-address 10.10.0.94 version 1preferred
 interval 100
```

The following example shows SNTP enabled with the **server-address** parameter configured.

```
ALU-1>config>system>time# info
----------------------------------------------
        sntp
            server-address 10.10.0.94 version 1 preferred interval 100
            no shutdown
        exit
        dst-zone PT start-date 2018/04/04 12:00 end-date 2018/10/25 12:00
        zone GMT
----------------------------------------------
ALU-1>config>system>time#
```

6.10.1.2.5 PTP

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard *1588 2008*. PTP provides the capability to synchronize network elements to a Stratum-1 clock or primary reference clock (PRC) traceable source over a network that may or may not be PTP-aware.

The **ptp** command specifies the PTP source as an option for recovered time. The specific PTP clock is identified by *clock-id* (from 1 to 16 for PTP clocks that use IPv4 or IPv6 encapsulation, and **csm** for PTP clocks that use Ethernet encapsulation) and has an assigned *priority-value* (from 1 to 16).

CLI syntax:
```
config>system>time
    ptp
        clock clock-id time-ref-priority priority-value
        clock csm time-ref-priority priority-value
```

Example:
```
config>system>time# ptp
config>system>time>ptp# clock 1 time-ref-priority 1
```

6.10.1.2.6 Time-of-day measurement (ToD-1pps)

The 7705 SAR can receive and extract time of day/phase recovery from a 1588 grandmaster clock or boundary clock and transmit the recovered time of day/phase signal to an external device such as a base station through an external time of day port, where available. Transmission is through the ToD or ToD/PPS Out port with a 1 pulse/s output signal. The port interface communicates the exact time of day by the rising edge of the 1 pulse/s signal.

The **tod-1pps** command specifies the format for the time of day (ToD) message that is transmitted out the ToD or ToD/PPS Out port and specifies whether the 1pps output is enabled.

CLI syntax:

```
config>system>time
    tod-1pps
        message-type {ct | cm | irig-b002-b122 | irig-b003-b123 | irig-
b006-b126 | irig-b007-b127}
        output
```

Example:

```
config>system>time# tod-1pps
config>system>time>tod-1pps# message-type ct
config>system>time>tod-1pps# output
```

6.10.1.2.7 GNSS

For a 7705 SAR chassis that is equipped with a GNSS receiver and an attached GNSS antenna, the GNSS receiver can be used as a synchronous timing source. GNSS data is used to provide network-independent frequency and ToD synchronization.

The **gnss** command specifies a GNSS receiver port as a synchronous timing source. The specific GNSS receiver port is identified by *port-id* and has an assigned *priority-value* (from 1 to 16).

CLI syntax:

```
config>system>time
    gnss
        port port-id time-ref-priority priority-value
```

Example:

```
config>system>time# gnss
config>system>time>gnss# port 1/2/1 time-ref-priority 1
```

6.10.1.2.8 CRON

The **cron** command is used for periodic and date- and time-based scheduling.

The schedule function configures the type of schedule to run, including one-time-only (one-shot), periodic, or calendar-based runs. All runs are scheduled by month, day, hour, minute, and interval (seconds). If **end-time** and **interval** are both configured, whichever condition is reached first is applied.

CLI syntax:

```
config>system>cron
    schedule schedule-name [owner schedule-owner]
        count number
        day-of-month {day-number [..day-number] | all}
        description description-string
        end-time [date | day-name] time
        hour {hour-number [..hour-number] | all}
        interval seconds
        minute {minute-number [..minute-number] | all}
        month {month-number [..month-number] | month-name [..month-name] |
  all}
        script-policy policy-name [owner policy-owner]
        type schedule-type
```

```
            weekday {weekday-number [..weekday-number] | day-name [..day-name]
    | all}
            no shutdown
```

The following example creates a schedule named "test2" to run a script policy named "test_policy" every 15 minutes on the 17th of each month and every Friday until noon on December 17, 2018:

Example:

```
config>system>cron# schedule test2
config>system>cron>sched# day-of-month 17
config>system>cron>sched# end-time 2018/12/17 12:00
config>system>cron>sched# minute 0 15 30 45
config>system>cron>sched# weekday friday
config>system>cron>sched# script-policy "test_policy"
config>system>cron>sched# no shutdown
```

6.10.2 Configuring script parameters

The 7705 SAR provides centralized script management for CLI scripts that are used by CRON and the Event Handling System (EHS). Scripts contain a set of CLI commands that are executed at a scheduled time or when an event is triggered.

The **script** and **script-policy** commands within the **config>system>script-control** context configure the script parameters.

The **script** command assigns a name to the script and references its location. When the script has been defined, a **script-policy** is configured that calls the previously configured script. The **script-policy** also specifies a location and filename that stores the results of the script run.

CLI syntax:

```
config>system
    script-control
        script script-name [owner script-owner]
            description description-string
            location file-url
            no shutdown
        script-policy policy-name [owner policy-owner]
            expire-time {seconds | forever}
            lifetime {seconds | forever}
            max-completed unsigned
            results file-url
            script script-name [owner script-owner]
            no shutdown
```

Example:

```
config>system# script-control
config>system>script-control# script "test_script"
config>system>script-control>script# location "cf3:/test.txt"
config>system>script-control>script# no shutdown
config>system>script-control>script# exit
config>system>script-control# script-policy "test_policy"
config>system>script-control>script-policy# results "cf3:/script-
results.txt"
config>system>script-control>script-policy# max-completed 4
config>system>script-control>script-policy# expire-time 7200
config>system>script-control>script-policy# no shutdown
config>system>script-control>script-policy# exit
```

```
config>system>script-control># exit
```

The following displays the configuration:

```
Dut-B>config>system>script-control# info
----------------------------------------------
        script "test_script"
            location "cf3:/test.txt"
            no shutdown
        exit
        script-policy "test_policy"
            results "cf3:/script-results.txt"
            script "test_script"
            max-completed 4
            expire-time 7200
            no shutdown
        exit
----------------------------------------------
Dut-B>config>system>script-control#
```

6.10.3 Configuring synchronization and redundancy

Use the CLI syntax displayed below to configure various synchronization and redundancy parameters:

- Configuring synchronization
- Configuring manual synchronization
- Forcing a switchover
- Configuring synchronization options
- Configuring multi-chassis redundancy

6.10.3.1 Configuring synchronization

The **switchover-exec** command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CSM card.

CLI syntax:
```
config>system
    switchover-exec file-url
```

6.10.3.2 Configuring manual synchronization

Automatic synchronization can be configured in the **config>system> synchronization** context.

Manual synchronization can be configured with the following command:

CLI syntax:
```
admin
    redundancy
```

```
                                    synchronize {boot-env | config}
```

Example:

```
admin>redundancy# synchronize config
```

The following shows the output that displays during a manual synchronization:

```
ALU-1>admin>redundancy# synchronize config

Syncing configuration......

Syncing configuration.....Completed.
ALU-1#
```

6.10.3.3 Forcing a switchover

The **force-switchover now** command forces an immediate switchover to the standby CSM card.

CLI syntax:

```
admin
    redundancy
        force-switchover [now]
```

Example:

```
admin>redundancy# force-switchover now
```

```
ALU-1# admin redundancy force-switchover now
ALU-1y#
Resetting...
?
```

If the active and standby CSMs are not synchronized for some reason, users can manually synchronize the standby CSM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CSM.

6.10.3.4 Configuring synchronization options

Network operators can specify the type of synchronization operation to perform between the primary and secondary CSMs after a change has been made to the configuration files or the boot environment information contained in the BOF.

Use the following CLI command to configure the **boot-env** option:

CLI syntax:

```
config
    redundancy
        synchronize {boot-env | config}
```

Example:

```
config>redundancy# synchronize boot-env
```

The following displays the configuration:

```
*ALU-1>config>redundancy# synchronize boot-env
*ALU-1>config>redundancy# show redundancy synchronization
===============================================================================
Synchronization Information
===============================================================================
Standby Status              : disabled
Last Standby Failure        : N/A
Standby Up Time             : N/A
Failover Time               : N/A
Failover Reason             : N/A
Boot/Config Sync Mode       : Boot Environment
Boot/Config Sync Status     : No synchronization
Last Config File Sync Time  : Never
Last Boot Env Sync Time     : Never
===============================================================================
```

Use the following CLI command to configure the **config** option:

CLI syntax:
```
config
    redundancy
        synchronize {boot-env | config}
```

Example:
```
config>redundancy# synchronize config
```

The following example displays the configuration.

```
ALU-1>config>redundancy# synchronize config
ALU-1>config>redundancy# show redundancy synchronization
=================================================
Synchronization Information
=================================================
Synchronize Mode       : Configuration
Synchronize Status     : No synchronization
Last Config Sync Time  : 2006/06/27 09:17:15
Last Boot Env Sync Time : 2006/06/24 07:16:37
=================================================
```

6.10.3.5 Configuring multi-chassis redundancy

When configuring multi-chassis redundancy, configuration must be performed on the two nodes that forms redundant-pair peer nodes. Each node points to its peer using the peer command.

When creating a multi-chassis LAG, the LAG must first be created under the **config>lag** *lag-id* context. Additionally, the LAG must be in access mode and LACP must be enabled (active or passive). Under the **multi-chassis>peer>mc-lag** context, the *lag-id* is the ID of the previously created LAG.

Use the following CLI syntax to configure multi-chassis redundancy features:

CLI syntax:
```
config>redundancy
    multi-chassis
        peer ip-address
            authentication-key [authentication-key | hash-key] [hash |
 hash2]
```

```
                    description description-string
                    mc-lag
                    hold-on-neighbor-failure multiplier
                    keep-alive-interval interval
                    lag lag-id lacp-key admin-key system-id system-id [remote-
lag lag-id] system-priority system-priority
                    no shutdown
                    source-address ip-address
```

Example:

```
config>redundancy#
config>redundancy# multi-chassis
config>redundancy>multi-chassis# peer 10.10.10.2 create
config>redundancy>multi-chassis>peer# description "Mc-Lag peer 10.10.10.2"
config>redundancy>multi-chassis>peer# mc-lag
config>redundancy>mc>peer>mc-lag# lag 1 lacp-key 32666 system-id
 00:00:00:33:33:33 system-priority 32888
config>redundancy>mc>peer>mc-lag# no shutdown
config>redundancy>mc>peer>mc-lag# exit
config>redundancy>multi-chassis>peer# no shutdown
config>redundancy>multi-chassis>peer# exit
config>redundancy>multi-chassis# exit
config>redundancy#
```

The following displays the configuration:

```
A:7705:Dut-A>config>redundancy# info
----------------------------------------------
            multi-chassis
                peer 10.10.10.2 create
                    description "Mc-Lag peer 10.10.10.2"
                    mc-lag
                        lag 1 lacp-key 32666 system-id 00:00:00:33:33:33 system
priority 32888
                        no shutdown
                    exit
                    no shutdown
                exit
            exit
----------------------------------------------
A:7705:Dut-A>config>redundancy#
```

6.10.4 Configuring ATM parameters

The ATM context configures system-wide ATM parameters.

CLI syntax:

```
config>system
    atm
        atm-location-id location-id
```

Example:

```
config>system# atm
config>system>atm# atm-location-id
 03:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
```

The following example shows the ATM configuration.

```
ALU-1>config>system>atm# info
----------------------------------------------
            atm-location-id 03:00:00:00:00:00:00:00:00:00:00:00:00:00:00
exit
----------------------------------------------
ALU-1>config>system>atm#
```

6.10.5 Configuring backup copies

The **config-backup** command allows you to specify the maximum number of backup versions of configuration and index files kept in the primary location.

For example, if the **config-backup** *count* is set to 5 and the configuration file is called **xyz.cfg**, the file **xyz.cfg** is saved with a .1 extension when the **save** command is executed. Each subsequent **config-backup** command increments the numeric extension until the maximum count is reached. The oldest file (5) is deleted as more recent files are saved.

- xyz.cfg
- xyz.cfg.1
- xyz.cfg.2
- xyz.cfg.3
- xyz.cfg.4
- xyz.cfg.5
- xyz.ndx

Each persistent index file is updated at the same time as the associated configuration file. When the index file is updated, then the save is performed to **xyz.cfg** and the index file is created as **xyz.ndx**. Synchronization between the active and standby CSMs is performed for all configurations and their associated persistent index files.

CLI syntax:
```
config>system
    config-backup count
```

Example:
```
config>system#
config>system# config-backup 7
```

The following example shows the **config-backup** configuration.

```
ALU-1>config>system> info
#----------------------------------------
echo "System Configuration"
#----------------------------------------
        name "ALU-1"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        config-backup 7
...
```

```
-------------------------------------------
ALU-1>config>system>
```

6.10.6 Configuring system administration parameters

Use the CLI syntax displayed below to configure various system administration parameters.

Administrative parameters include:

- Disconnect
- Set-time
- Display-config
- Tech-support
- Save
- Reboot
- Post-boot configuration extension files

CLI syntax:

```
admin
    certificate
    clear
    compare
    debug-save
    disconnect [address ip-address | username user-name | session-
id session-id | {console | telnet | ftp | ssh | mct}]
    display-config [detail | index]
    enable-tech
    reboot [active | standby][upgrade][now]
    redundancy
    rollback
    save [file-url] [detail] [index]
    set-time date time
    system
    tech-support
    update
```

6.10.6.1 Disconnect

The **disconnect** command immediately disconnects a user from a console, Telnet, FTP, SSH, SFTP, or MPT craft terminal (MCT) session.

The **ssh** keyword disconnects users connected to the node via SSH or SFTP.

✎ **Note:** Configuration modifications are saved to the primary image file.

CLI syntax:

```
admin
```

```
        disconnect [address ip-address | username user-name | session-
id session-id | {console | telnet | ftp | ssh | mct}]
```

Example:

```
admin# disconnect
```

The following example displays the disconnect command results.

```
ALU-1>admin# disconnect
ALU-1>admin# Logged out by the administrator
Connection to host lost.
```

6.10.6.2 Set-time

Use the **set-time** command to set the system date and time. The time entered should be accurate for the time zone configured for the system. The system converts the local time to UTC before saving to the system clock which is always set to UTC. If SNTP or NTP is enabled (**no shutdown**), this command cannot be used. The **set-time** command does not take into account any daylight saving offset if defined.

CLI syntax:

```
admin
    set-time date time
```

Example:

```
admin# set-time 2010/09/24 14:10:00
```

The following example displays the **set-time** command results.

```
ALU-1# admin set-time 2010/09/24 14:10:00
ALU-1# show time
Fri Sept 24 14:10:25 UTC 2010
ALU-1#
```

6.10.6.3 Display-config

The **display-config** command displays the system's running configuration.

CLI syntax:

```
admin
    display-config [detail] [index]
```

Example:

```
admin# display-config detail
```

The following example displays a portion of the **display-config detail** command results.

```
ALU-1>admin# display-config detail
# TiMOS-B-0.0.current both/i386 NOKIA SAR 7705
# Copyright (c) 2016 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Fri Sept 24 01:32:43 EDT 2016 by csabuild in /rel0.0/I270/panos/main
```

```
# Generated FRI SEPT 24 14:48:31 2016 UTC

exit all
configure
#--------------------------------------
echo "System Configuration"
#--------------------------------------
    system
        name "ALU-1"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        config-backup 7
        boot-good-exec "ftp://*:*@xxx.xxx.xxx.xx/home/csahwreg17/images/env.cfg"
        no boot-bad-exec
        no switchover-exec
        snmp
            engineID "0000197f00006883ff000000"
            packet-size 1500
            general-port 161
            no shutdown
        exit
        login-control
            ftp
                inbound-max-sessions 3
            exit
            ssh
                no disable-graceful-shutdown
                inbound-max-sessions 5
                outbound-max-sessions 5
                ttl-security 100
            exit
            telnet
                no enable-graceful-shutdown
                inbound-max-sessions 5
                outbound-max-sessions 5
                ttl-security 50
            exit
            idle-timeout 1440
            pre-login-message "Property of Service Routing Inc.Unauthorized access
prohibited."
            motd text "Notice to all users: Software upgrade scheduled 3/2 1:00 AM"
            login-banner
            no exponential-backoff
        exit
        atm
            no atm-location-id
        exit
        security
            management-access-filter
                default-action permit
                entry 1
                    no description
...
ALU-1>admin#
```

6.10.6.4 Tech-support

The **tech-support** command creates a system core dump.

> **Note:** This command should only be used with explicit authorization and direction from the Nokia Technical Assistance Center (TAC).

6.10.6.5 Save

The **save** command saves the running configuration to a configuration file. When the **debug-save** parameter is specified, debug configurations are saved in the config file. If this parameter is not specified, debug configurations are not saved between reboots.

CLI syntax:

```
admin
    save [file-url] [detail] [index]
    debug-save [file-url]
```

Example:

```
admin# save ftp://test:test@192.168.x.xx/./1.cfg
admin# debug-save debugsave.txt
```

The following example displays the **save** command results.

```
ALU-1>admin# save ftp://test:test@192.168.x.xx/./1x.cfg
Writing file to ftp://test:test@192.168.x.xx/./1x.cfg
Saving configuration ...Completed.
ALU-1>admin# debug-save ftp://test:test@192.168.x.xx/./debugsave.txt
Writing file to ftp://julie:julie@192.168.x.xx/./debugsave.txt
Saving debug configuration .....Completed.
```

6.10.6.6 Reboot

The **reboot** command reboots the router, including redundant CSMs in redundant systems. If the **now** option is not specified, you are prompted to confirm the reboot operation. The **reboot upgrade** command forces an upgrade of the boot ROM and a reboot.

CLI syntax:

```
admin
    reboot [active | standby] | [upgrade] [now]
```

Example:

```
admin# reboot now
```

If synchronization fails, the standby does not reboot automatically. The **show redundancy synchronization** command displays synchronization output information.

6.10.6.7 Post-boot configuration extension files

Two post-boot configuration extension files are supported and are triggered when either a successful or failed boot configuration file is processed. The commands specify URLs for the CLI scripts to be run following the completion of the boot-up configuration. A URL must be specified or no action is taken.

The commands are persistent between router (re)boots and are included in the configuration saves (**admin>save**).

CLI syntax:

```
config>system
    boot-bad-exec file-url
    boot-good-exec file-url
```

Example:

```
config>system# boot-bad-exec ftp://t:t@192.168.xx.xxx/./
fail.cfg
config>system# boot-good-exec
ftp://test:test@192.168.xx.xxx/./
ok.cfg
```

The following example displays the command output:

```
ALU-1>config>system# info
#----------------------------------------
echo "System Configuration"
#----------------------------------------
        name "ALU-1"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        config-backup 7
        boot-good-exec "ftp://test:test@192.168.xx.xxx/./ok.cfg"
        boot-bad-exec "ftp://test:test@192.168.xx.xxx/./fail.cfg"
        sync-if-timing
            begin
            ref-order ref1 ref2 bits
..
----------------------------------------------
ALU-1>config>system#
```

6.10.6.7.1 Show command output and console messages

The **show>system>information** command displays the current value of the bad/good exec URLs and indicates whether a post-boot configuration extension file was executed when the system was booted. If an extension file was executed, the **show>system> information** command also indicates if it completed successfully or not.

```
7705:Dut-A# show system information

===============================================================================
System Information
===============================================================================
System Name            : 7705:Dut-A
System Type            : 7705 SAR-8 v2
Chassis Topology       : Standalone
System Version         : B-0.0.I346
Crypto Module Version  : SRCM 3.0
System Contact         : Fred Information Technology
System Location        : Bldg.1-floor 2-Room 201
System Coordinates     : N 45 58 23, W 34 56 12
System Active Slot     : A
System Up Time         : 1 days, 02:03:17.62 (hr:min:sec)
```

```
SNMP Port            : 161
SNMP Engine ID       : 0000197f000000164d3c3910
SNMP Engine Boots    : 58
SNMP Max Message Size : 1500
SNMP Admin State     : Enabled
SNMP Oper State      : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State      : OK

Tel/Tel6/SSH/FTP Admin : Enabled/Disabled/Enabled/Enabled
Tel/Tel6/SSH/FTP Oper  : Up/Down/Up/Up

BOF Source           : cf3:
Image Source         : primary
Config Source        : primary
Last Booted Config File: cf3:/config.cfg
Last Boot Cfg Version  : FRI APR 20 16:24:27 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I346 both/i386 NOKIA SAR 7705
                         # Copyright (c) 2016 Nokia. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Tue Mar 11 01:43:47 EDT 2016 by
                         csabuild in /rel0.0/I346/panos/main # Generated TUE
                         MAR 11 20:00:37 2016 UTC
Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-0.0.I346 both/i386 NOKIA SAR 7705
                         # Copyright (c) 2016 Nokia. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Tue Mar 11 01:43:47 EDT 2016 by
                         csabuild in /rel0.0/I346/panos/main # Generated TUE
                         MAR 11 20:00:37 2016 UTC
Last Saved Config    : N/A
Time Last Saved      : N/A
Changes Since Last Save: Yes
User Last Modified   : admin
Time Last Modified   : 2016/03/25 10:03:09
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script        : N/A
Cfg-OK Script Status  : not used
Cfg-Fail Script      : N/A
Cfg-Fail Script Status : not used

Microwave S/W Package  : invalid

Management IP Addr   : 192.168.1.202/16
Primary DNS Server   : 192.168.x.x
Secondary DNS Server  : N/A
Tertiary DNS Server   : N/A
DNS Domain           : domain.com
DNS Resolve Preference : ipv4-only
BOF Static Routes    :
  To                 Next Hop
  192.168.0.0/16     192.168.1.1
ATM Location ID      : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ATM OAM Retry Up     : 2
ATM OAM Retry Down   : 4
ATM OAM Loopback Period: 10

ICMP Vendor Enhancement: Disabled
Eth QinQ untagged SAP  : False
===============================================================================
7705:Dut-A#
```

When executing a post-boot configuration extension file, status messages are output to the console screen before the "Login" prompt.

The following is an example of a failed boot-up configuration that caused a boot-bad-exec file containing another error to be executed:

```
Attempting to exec configuration file:
'ftp://test:test@192.168.xx.xxx/./12.cfg' ...
System Configuration
Log Configuration
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./12.cfg, Line 195: Command "log" failed.
CRITICAL: CLI #1002 An error occurred while processing the configuration file.
The system configuration is missing or incomplete.
MAJOR: CLI #1008 The SNMP daemon is disabled.
If desired, enable SNMP with the 'config>system>snmp no shutdown' command.
Attempting to exec configuration failure extension file:
'ftp://test:test@192.168.xx.xxx/./fail.cfg' ...
Config fail extension
Enabling SNMP daemon
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./fail.cfg, Line 5: Command "abc log" failed.
TiMOS-B-5.0.R3 both/hops Nokia 7705 SAR Copyright (c) 2018 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Feb 18 12:45:00 EST 2018 by builder in /re8.0/b1/R3/panos/main
```

6.10.7 System timing

If network timing is required for the synchronous interfaces in a 7705 SAR, a timing subsystem is used to provide a Stratum 3 quality clock to all synchronous interfaces within the system. The clock source is specified in the **config>port>tdm>ds1 | e1> clock-source** context.

This section describes the commands used to configure and control the timing subsystem.

- Entering edit mode
- Configuring timing references
- Configuring IEEE 1588v2 PTP
- Configuring QL values for SSM
- Using the revert command
- Other editing commands
- Forcing a specific reference

CLI syntax:
```
config>system>sync-if-timing
    abort
    begin
    commit
    external
        input-interface
            impedance {high-impedance | 50-ohm | 75-ohm}
            type {2048khz-G703 | 5mhz | 10mhz}
        output-interface
            type {2048khz-G703 | 5mhz | 10mhz}
    ref-order first second [third]
    ref1
        source-port port-id [adaptive]
```

```
            no shutdown
        ref2
            source-port port-id [adaptive]
            no shutdown
        revert
```

6.10.7.1 Entering edit mode

To enter the mode to edit timing references, you must enter the **begin** keyword at the **config>system>sync-if-timing**# prompt.

Use the following CLI syntax to enter the edit mode:

CLI syntax:
```
config>system>sync-if-timing
    begin
```

The following error message displays when you try to modify **sync-if-timing** parameters without entering **begin** first.

```
ALU-1>config>system>sync-if-timing>ref1# source-port 1/1/1
MINOR: CLI The sync-if-
timing must be in edit mode by calling begin before any changes can be made.
MINOR: CLI Unable to set source port for ref1 to 1/1/1.
ALU-1>config>system>sync-if-timing>ref1#
```

6.10.7.2 Configuring timing references

The following example shows the command usage:

Example:
```
config>system# sync-if-timing
config>system>sync-if-timing# begin
config>system>sync-if-timing# ref1
config>system>sync-if-timing>ref1# source-port1/1/1
config>system>sync-if-timing>ref1# no shutdown
config>system>sync-if-timing>ref1# exit
config>system>sync-if-timing# ref2
config>system>sync-if-timing>ref2# source-port1/1/2
config>system>sync-if-timing>ref2# no shutdown
config>system>sync-if-timing>ref2# exit
config>system>sync-if-timing>commit
```

The following displays the timing reference parameters:

```
ALU-1>config>system>sync-if-timing# info
----------------------------------------------
        ref-order ref2 ref1
        ref1
            source-port 1/1/1
            no shutdown
        exit
        ref2
            no shutdown
            source-port 1/1/2
```

```
            exit
```

6.10.7.3 Configuring IEEE 1588v2 PTP

Use the following CLI syntax to configure basic IEEE 1588v2 PTP parameters.

CLI syntax:

```
config>system>ptp
    clock clock-id [create]
        clock-mda mda-id
        clock-type {ordinary [master | slave] | boundary | transparent-
e2e}
        domain domain-value
        dynamic-peers
        priority1 priority-value
        priority2 priority-value
        profile ieee1588-20008
        ptp-port port-id
            anno-rx-timeout number-of-timeouts
            log-anno-interval log-anno-interval
            log-sync-interval log-sync-interval
            peer peer-id ip-address {ip-address | ipv6-address}
            [no] shutdown
            unicast-negotiate
        [no] shutdown
        source-interface ip-if-name
```

```
config>system>sync-if-timing
    ref1
        source-ptp-clock clock-id
    ref2
        source-ptp-clock clock-id
```

The following example shows the command usage:

Example:

```
config>system# ptp clock 1 create
config>system>ptp>clock# clock-type ordinary slave
config>system>ptp>clock# source-interface ptp-loop
config>system>ptp>clock# clock-mda 1/2
config>system>ptp>clock# domain 0
config>system>ptp>clock# no dynamic-peers
config>system>ptp>clock# priority1 128
config>system>ptp>clock# priority2 128
config>system>ptp>clock# profile ieee1588-2008
config>system>ptp>clock# ptp-port 1
config>system>ptp>clock>ptp-port# anno-rx-timeout 3
config>system>ptp>clock>ptp-port# log-anno-interval 1
config>system>ptp>clock>ptp-port# log-sync-interval -6
config>system>ptp>clock>ptp-port# unicast-negotiate
config>system>ptp>clock>ptp-port# peer 1
config>system>ptp>clock>ptp-port>peer# description "Peer to Boundary
 Clock"
config>system>ptp>clock>ptp-port>peer# ip-address 10.222.222.10
config>system>ptp>clock>ptp-port>peer# exit
config>system>ptp>clock>ptp-port# peer 2
config>system>ptp>clock>ptp-port>peer# description ToGM
config>system>ptp>clock>ptp-port>peer# ip-address 192.168.2.10
config>system>ptp>clock>ptp-port>peer# exit
config>system>ptp>clock>ptp-port# no shutdown
```

```
config>system>ptp>clock>ptp-port# exit
config>system>ptp>clock# no shutdown
config>system>ptp>clock# exit
config>system>ptp# exit
config>system# sync-if-timing begin
config>system>sync-if-timing# ref1
config>system>sync-if-timing>ref1# source-ptp-clock 1
config>system>sync-if-timing>ref1# no shutdown
config>system>sync-if-timing>ref1# exit
```

The following display shows a basic IEEE 1588v2 PTP configuration:

```
ALU-1>config>system>ptp># info
#-------------------------------------------------
echo "System IEEE 1588 PTP Configuration"
#-------------------------------------------------
    system
        ptp
            clock 1 create
                clock-type ordinary slave
                source-interface "ptp loop"
                clock-mda 1/2
                domain 0
                no dynamic-peers
                priority1 128
                priority2 128
                profile ieee1588-2008
                ptp-port 1
                    anno-rx-timeout 3
                    log-anno-interval 1
                    log-sync-interval -6
                    unicast-negotiate
                    peer 1
                        description "Peer to Boundary Clock"
                        ip-address 10.222.222.10
                    exit
                    peer 2
                        description "ToGM"
                        ip-address 192.168.2.10
                    exit
                    no shutdown
                exit
                no shutdown
            exit
        exit
    exit
```

6.10.7.4 Configuring QL values for SSM

Use the following syntax to configure the quality level (QL) values for Synchronization Status Messaging (SSM).

CLI syntax:
```
config>system>sync-if-timing
    abort
    begin
    external
        input-interface
            impedance {high-impedance | 50-ohm | 75-ohm}
            no shutdown
```

```
                ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc |
    ssu-a | ssu-b | sec | eec1 | eec2}
                type {2048khz-G703 | 5mhz | 10mhz}
        commit
        bits
            input
                [no] shutdown
            interface-type {ds1[{esf|sf}] | e1[{pcm30crc | pcm31crc}] |
    2048khz-G703}
            output
                line-length {110|220|330|440|550|660}
                [no] shutdown
            ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-
    a | ssu-b | sec | eec1 | eec2}
            ssm-bit sa-bit
                [no] shutdown
            ql-selection
            ref-order first second [third]
            ref1
                ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc |
    ssu-a | ssu-b | sec | eec1 | eec2}
                source-port port-id adaptive
                no shutdown
            ref2
                ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc |
    ssu-a | ssu-b | sec | eec1 | eec2}
                source-port port-id adaptive
                no shutdown
```

The following example shows the command usage:

Example:

```
config>system# sync-if-timing
config>system>sync-if-timing# begin
config>system>sync-if-timing# external
config>system>sync-if-timing>external# input-interface
config>system>sync-if-timing>external>input-interface# impedance 50-Ohm
config>system>sync-if-timing>external>input-interface# no shutdown
config>system>sync-if-timing>external>input-interface# ql-override prs
config>system>sync-if-timing>external>input-interface# exit
config>system>sync-if-timing>external# exit
config>system>sync-if-timing# commit
config>system>sync-if-timing# bits
config>system>sync-if-timing>bits# interface-type 2048khz-G703
config>system>sync-if-timing>bits# ssm-bit 8
config>system>sync-if-timing>bits# output
config>system>sync-if-timing>bits>output# line-length 220
config>system>sync-if-timing>bits>output# no shutdown
config>system>sync-if-timing>bits>output# exit
config>system>sync-if-timing>bits# ql-override prs
config>system>sync-if-timing>bits# exit
config>system>sync-if-timing# ql-selection
config>system>sync-if-timing# ref1
config>system>sync-if-timing>ref1# shutdown
config>system>sync-if-timing>ref1# ql-override prs
config>system>sync-if-timing>ref1# exit
config>system>sync-if-timing# ref2
config>system>sync-if-timing>ref2# no shutdown
config>system>sync-if-timing>ref2# ql-override prs
config>system>sync-if-timing>ref2# exit
config>system>sync-if-timing# exit
```

The following display shows a basic SSM QL configuration for the 7705 SAR-8 Shelf V2:

```
ALU-1>config>system>sync-if-timing# info
-----------------------------------------------
ref-order external ref1 ref2
            ql-selection
            external
                input-interface
                    no shutdown
                    impedance 50-Ohm
                    type 2048Khz-G703
                    ql-override prs
                exit
                output-interface
                    type 2048Khz-G703
                exit
            exit
            ref1
                no shutdown
                no source-port
                ql-override prs
            exit
            ref2
                no shutdown
                no source-port
                ql-override prs
            exit
            no revert
-----------------------------------------------
*ALU-1>>config>system>sync-if-timing#
```

The following display shows a basic SSM QL configuration for the 7705 SAR-18:

```
ALU-1>config>system>sync-if-timing# info
-----------------------------------------------
ref-order external ref1 ref2
            ql-selection
            exit
            bits
                interface-type 2048Khz-G703
                ssm-bit 8
                ql-override prs
                output
                    line-length 220
                    no shutdown
                exit
            ref1
                no shutdown
                no source-port
                ql-override prs
            exit
            ref2
                no shutdown
                no source-port
                ql-override prs
            exit
            no revert
-----------------------------------------------
```

6.10.7.5 Using the revert command

The **revert** command allows the clock to revert to a higher-priority reference if the current reference goes offline or becomes unstable. With revertive switching enabled, the highest-priority valid timing reference is used. If a reference with a higher priority becomes valid, a reference switchover to that reference initiates. If a failure on the current reference occurs, the next highest reference takes over.

With non-revertive switching, the active reference always remains selected while it is valid, even if a higher-priority reference becomes available. If this reference becomes invalid, a reference switchover to a valid reference with the highest priority initiates. When the failed reference becomes operational, it is eligible for selection.

CLI syntax:
```
config>system>sync-if-timing
    revert
```

6.10.7.6 Other editing commands

Other editing commands include:

- **commit** — saves changes made to the timing references during a session Modifications are not persistent across system boots unless this command is entered.

- **abort** — discards changes that have been made to the timing references during a session

CLI syntax:
```
config>system>sync-if-timing
    abort
    commit
```

6.10.7.7 Forcing a specific reference

You can force the system synchronous timing output to use a specific reference.

> **Note:** The **debug sync-if-timing force-reference** command should only be used to test and debug problems. After the system timing reference input has been forced, it does not revert to another reference unless explicitly reconfigured.

When the command is executed, the current system synchronous timing output is immediately referenced from the specified reference input. If the specified input is not available (shut down), or in a disqualified state, the timing output enters a holdover state based on the previous input reference.

Debug configurations are not saved between reboots.

CLI syntax:
```
debug>sync-if-timing
    force-reference {external | ref1 | ref2}
```

Example:
```
debug>sync-if-timing# force-reference
```

6.11 Configuring system monitoring thresholds

6.11.1 Creating events

The **event** command controls the generation and notification of threshold crossing events configured with the **alarm** command. When a threshold crossing event is triggered, the **rmon event** configuration optionally specifies whether an entry in the RMON-MIB log table is created to record the occurrence of the event. It can also specify whether an SNMP notification (trap) is generated for the event. There are two notifications for threshold crossing events, a rising alarm and a falling alarm.

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the 7705 SAR event logs. However, when the event is set to trap, the generation of a rising alarm or falling alarm notification creates an entry in the 7705 SAR event logs and that is distributed to whatever 7705 SAR log destinations are configured: console, session, memory, file, syslog, or SNMP trap destination. The 7705 SAR logger message includes a rising or falling threshold crossing event indicator, the sample type (absolute or delta), the sampled value, the threshold value, the *rmon-alarm-id*, the associated *rmon-event-id* and the sampled SNMP object identifier.

The **alarm** command configures an entry in the RMON-MIB alarm table. The **alarm** command controls the monitoring and triggering of threshold crossing events. In order for notification or logging of a threshold crossing event to occur there must be at least one associated **rmon event** configured.

The agent periodically takes statistical sample values from the MIB variable specified for monitoring and compares them to thresholds that have been configured with the **alarm** command. The **alarm** command configures the MIB variable to be monitored, the polling period (interval), sampling type (absolute or delta value), and rising and falling threshold parameters. If a sample has crossed a threshold value, the associated 'event' is generated.

Preconfigured CLI threshold commands are available. Preconfigured commands hide some of the complexities of configuring RMON alarm and event commands and perform the same functions. In particular, the preconfigured commands do not require the user to know the SNMP object identifier to be sampled. The preconfigured threshold configurations include memory warnings, alarms, and compact flash usage warnings and alarms.

To create events, use the following CLI syntax:

CLI syntax:
```
config>system
    thresholds
        cflash-cap-alarm cflash-id rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-
alarm alarm-type]
        cflash-cap-warn cflash-id rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-
alarm alarm-type]
        memory-use-alarm rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-
alarm alarm-type]
        memory-use-warn rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-
alarm alarm-type]
            rmon
                alarm rmon-alarm-id variable-oid oid-string interval seconds
 [sample-type] [startup-alarm alarm-type] [rising-event rmon-event-
id rising-threshold threshold] [falling-event rmon-event-id falling-
threshold threshold] [owner owner-string]
```

```
                      event rmon-event-id [event-type] [description description-
           string] [owner owner-string]
```

Example:

```
config>system>thresholds# cflash-cap-warn cf3-B: rising-threshold 2000000
 falling-threshold 1999900 interval 240 trap startup-alarm either
config>system>thresholds# memory-use-alarm rising-threshold 50000000
 falling-threshold 45999999 interval 500 both startup-alarm either
config>system>thresholds# rmon
config>system>thresholds>rmon# event 5 both description "alarm testing"
 owner "Timos CLI"
```

The following example displays the command output:

```
A:ALU-49>config>system>thresholds# info
----------------------------------------------
            rmon
                event 5 description "alarm testing" owner "Timos CLI"
            exit
            cflash-cap-warn cf1-B: rising-threshold 2000000 falling-
             threshold 1999900 interval 240 trap
            memory-use-alarm rising-threshold 50000000 falling-threshold 45999999
             interval 500
----------------------------------------------
A:ALU-49>config>system>thresholds#
```

6.12 Configuring LLDP

Use the following syntax to configure LLDP:

CLI syntax:

```
config>system>lldp
    message-fast-tx time
    message-fast-tx-init count
    notification-interval time
    reinit-delay time
    tx-credit-max count
    tx-hold-multiplier multiplier
    tx-interval interval
```

Example:

```
config>system# lldp
config>system>lldp# message-fast-tx 100
config>system>lldp# notification-interval 10
config>system>lldp# reinit-delay 5
config>system>lldp# tx-credit-max 20
config>system>lldp# tx-hold-multiplier 2
config>system>lldp# tx-interval 10
```

The following example shows the system LLDP configuration:

```
A:ALU-49>config>system>lldp# info
----------------------------------------------
tx-interval 10
tx-hold-multiplier 2
reinit-delay 5
```

```
notification-interval 10
tx-credit-max 20
message-fast-tx 100
-----------------------------------------------
A:ALU-49>config>system>lldp#
```

6.13 System command reference

6.13.1 Command hierarchies

-

6.13.1.1 Configuration commands

6.13.1.1.1 System information and general commands

```
config
    - system
        - atm
            - atm-location-id location-id
            - no atm-location-id
        - boot-bad-exec file-url
        - no boot-bad-exec
        - boot-good-exec file-url
        - no boot-good-exec
        - clli-code clli-code
        - no clli-code
        - config-backup  count
        - no config-backup
        - contact contact-name
        - no contact
        - coordinates coordinates
        - no coordinates
        - fp
```

```
                   - options
                        - vpls-high-scale
                              - [no] shutdown
            - [no] identifier id
            - load-balancing
                  - [no] l4-load-balancing
                  - lsr-load-balancing hashing-algorithm [bottom-of-stack hashing-treatment] [use-
ingress-port]
                  - no lsr-load-balancing
                  - [no] system-ip-load-balancing
            - location location
            - no location
            - name system-name
            - no name
            - [no] power-feed-monitoring {A | B | C}
            - spt
                  - security-aggregate-rate agg-rate (refer to the Interface Configuration Guide,
 "Adapter Card Commands" for information)
                  - no security-aggregate-rate (refer to the Interface Configuration Guide, "Adapter
 Card Commands" for information)
```

6.13.1.1.2 System alarm commands

```
config
    - system
        - thresholds
            - cflash-cap-alarm cflash-id rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-alarm alarm-type]
            - no cflash-cap-alarm cflash-id
            - cflash-cap-warn cflash-id rising-threshold threshold [falling-
threshold threshold] interval seconds [rmon-event-type] [startup-alarm alarm-type]
            - no cflash-cap-warn cflash-id
            - memory-use-alarm rising-threshold threshold [falling-threshold threshold]
 interval seconds [rmon-event-type] [startup-alarm alarm-type]
            - no memory-use-alarm
            - memory-use-warn rising-threshold threshold [falling-threshold threshold]
 interval seconds [rmon-event-type] [startup-alarm alarm-type]
            - no memory-use-warn
            - [no] rmon
                - alarm rmon-alarm-id variable-oid oid-string interval seconds [sample-type]
[startup-alarm alarm-type] [rising-event rmon-event-id rising-threshold threshold] [falling
event rmon-event-id falling-threshold threshold] [owner owner-string]
                    - no alarm rmon-alarm-id
                - event rmon-event-id [event-type] [description description-string]
[owner owner-string]
                    - no event rmon-event-id
```

6.13.1.1.3 Persistence commands

```
config
    - system
        - persistence
            - dhcp-server
                - description description-string
                - no description
                - location cflash-id
                - no location
```

© 2024 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

6.13.1.1.4 System time commands

```
root
    - admin
        - set-time [date] [time]
config
    - system
        - time
            - [no] dst-zone [std-zone-name | non-std-zone-name]
                - end {end-week} {end-day} {end-month} [hours-minutes]
                - offset offset
                - start {start-week} {start-day} {start-month} [hours-minutes]
            - gnss
                - port port-id time-ref-priority priority-value
                - no port
            - [no] ntp
                - [no] authentication-check
                - authentication-key key-id key key [hash | hash2] type {des | message-digest}
                - no authentication-key key-id
                - broadcast  [router router-name] {interface ip-int-name} [key-id key-id]
  [version version] [ttl ttl]
                - no broadcast  [router router-name] {interface ip-int-name}
                - broadcastclient [router router-name] {interface ip-int-name} [authenticate]
                - no broadcastclient [router router-name] {interface ip-int-name}
                - [no] mda-timestamp
                - multicast [key-id key-id] [version version]
                - no multicast
                - multicastclient [authenticate]
                - no multicastclient
                - ntp-server  [authenticate]
                - no ntp-server
                - peer ip-address [key-id key-id] [version version] [prefer]
                - no peer ip-address
                - server {ip-address | system-time} [key-id key-id] [version version] [prefer]
                - no server {ip-address | system-time}
                - [no] shutdown
            - ptp
                - clock clock-id time-ref-priority priority-value
                - clock csm time-ref-priority priority-value
                - no clock
            - [no] sntp
                - [no] broadcast-client
                - server-address ip-address [version version-number] [normal | preferred]
  [interval seconds]
                - no server-address ip-address
                - [no] shutdown
            - tod-1pps
                - message-type {ct | cm | irig-b002-b122 | irig-b003-b123 | irig-b006-b126 |
  irig-b007-b127}
                - no message-type
                - [no] output
            - zone {std-zone-name | non-std-zone-name} [hh [:mm]]
            - no zone
```

6.13.1.1.5 CRON commands

```
config
    - system
        - cron
```

```
                    - [no] schedule schedule-name [owner schedule-owner]
                        - count number
                        - no count
                        - day-of-month {day-number [..day-number] | all}
                        - no day-of-month
                        - description description-string
                        - no description
                        - end-time [date | day-name] time
                        - no end-time
                        - hour {hour-number [..hour-number] | all}
                        - no hour
                        - interval seconds
                        - no interval
                        - minute {minute-number [..minute-number] | all}
                        - no minute
                        - month {month-number [..month-number] | month-name [..month-name] | all}
                        - no month
                        - script-policy policy-name [owner policy-owner]
                        - no script-policy
                        - [no] shutdown
                        - type schedule-type
                        - weekday {weekday-number [..weekday-number] | day-name [..day-name] | all}
                        - no weekday
```

6.13.1.1.6 Script control commands

```
config
    - system
        - script-control
            - [no] script script-name [owner script-owner]
                - description description-string
                - no description
                - location file-url
                - no location
                - [no] shutdown
            - [no] script-policy policy-name [owner policy-owner]
                - expire-time {seconds | forever}
                - lifetime {seconds | forever}
                - max-completed unsigned
                - results file-url
                - no results
                - script script-name [owner script-owner]
                - no script
                - [no] shutdown
```

6.13.1.1.7 System synchronization commands

```
config
    - system
        - sync-if-timing
            - abort
            - begin
            - bits
                - input
                    - [no] shutdown
                - interface-type {ds1 [{esf | sf}] | e1 [{pcm30crc | pcm31crc}] | 2048khz-G703}
                - no interface-type
                - output
```

```
                         - line-length {110 | 220 | 330 | 440 | 550 | 660}
                         - [no] shutdown
                         - source {line-ref | internal-clock}
                    - ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-a| ssu-b |
sec | eec1 | eec2}
                         - no ql-override
                         - ssm-bit sa-bit
                - commit
                - external
                    - input-interface
                         - impedance {high-impedance | 50-Ohm | 75-Ohm}
                         - [no] shutdown
                         - type {2048khz-G703 | 5mhz | 10mhz}
                         - no type
                    - output-interface
                         - type {2048khz-G703 | 5mhz | 10mhz}
                         - no type
                    - ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-a | ssu-b |
sec | eec1 | eec2}
                         - no ql-override
                - [no] ql-selection
                - ref-order first second [third]
                - no ref-order
                - ref1
                    - ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-a | ssu-b |
sec | eec1 | eec2}
                         - no ql-override
                         - [no] shutdown
                         - source-port port-id [adaptive]
                         - no source-port
                         - source-ptp-clock clock-id
                         - no source-ptp-clock
                - ref2
                    - ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-a | ssu-b |
sec | eec1 | eec2}
                         - no ql-override
                         - [no] shutdown
                         - source-port port-id [adaptive]
                         - no source-port
                         - source-ptp-clock clock-id
                         - no source-ptp-clock
            - [no] revert
```

6.13.1.1.8 System LLDP commands

```
config
    - system
        - lldp
            - message-fast-tx time
            - no message-fast-tx
            - message-fast-tx-init count
            - no message-fast-tx-init
            - notification-interval time
            - no notification-interval
            - reinit-delay time
            - no reinit-delay
            - tx-credit-max count
            - no tx-credit-max
            - tx-hold-multiplier multiplier
            - no tx-hold-multiplier
            - tx-interval interval
```

```
                - no tx-interval
```

6.13.1.1.9 System PTP commands

```
config
    - system
        - ptp
            - clock clock-id [create]
            - no clock
                - alternate-profile profile-name [create]
                - no alternate-profile profile-name
                    - description description-string
                    - no description
                    - domain domain-value
                    - no domain
                    - initial-time-inaccuracy initial-time-inaccuracy
                    - no initial-time-inaccuracy
                    - log-anno-interval log-anno-interval
                    - no log-anno-interval
                    - profile {c37dot238-2017 | iec-61850-9-3-2016}
                    - no profile
                - anno-rx-timeout number-of-timeouts
                - no anno-rx-timeout
                - [no] apts-asymmetry-compensation
                - clock-mda mda-id
                - no clock-mda
                - clock-type {ordinary {master | slave} | boundary | transparent-e2e}
                - no clock-type
                - domain domain-value
                - no domain
                - [no] dynamic-peers
                - freq-source {ptp | ssu}
                - no freq-source
                - local-priority priority
                - no local-priority
                - log-anno-interval log-anno-interval
                - no log-anno-interval
                - network-type {sdh | sonet}
                - no network-type
                - port port-id [create]
                - no port port-id
                    - address {01:1b:19:00:00:00 | 01:80:c2:00:00:0e}
                    - no address
                    - local-priority priority
                    - no local-priority
                    - log-delay-interval log-delay-interval
                    - no log-delay-interval
                    - log-sync-interval log-sync-interval
                    - no log-sync-interval
                    - master-only {true | false}
                    - profile {primary | name}
                    - no profile
                    - [no] shutdown
                    - time-inaccuracy-override time-inaccuracy-override
                    - no time-inaccuracy-override
                - priority1 priority-value
                - no priority1
                - priority2 priority-value
                - no priority2
                - profile {c37dot238-2017| iec-61850-9-3-2016 | ieee1588-2008 | itu-telecom-
freq | g8275dot1-2014 | g8275dot2-2016}
```

© 2024 Nokia.

```
                       - no profile
                       - ptp-port port-id
                            - anno-rx-timeout number-of-timeouts
                            - no anno-rx-timeout
                            - local-priority priority
                            - no local-priority
                            - log-anno-interval log-anno-interval
                            - no log-anno-interval
                            - log-sync-interval log-sync-interval
                            - no log-sync-interval
                            - master-only {true | false}
                            - peer peer-id
                                - description description-string
                                - no description
                                - ip-address {ip-address | ipv6-address}
                                - no ip-address
                            - [no] shutdown
                            - [no] unicast-negotiate
                       -  [no] shutdown
                       - source-interface ip-int-name
                       - no source-interface
                       - [no] tx-while-sync-uncertain
                       - [no] use-node-time
```

6.13.1.2 Administration commands

6.13.1.2.1 System administration commands

```
root
- admin
          - debug-save file-url
          - disconnect [address ip-address | username user-name |session-id session-id | {console
 | telnet | ftp | ssh | mct}]
          - display-config [detail | index]
          - [no] enable-tech
          - reboot [active | standby] | [upgrade] [now]
          - save [file-url] [detail] [index]
          - tech-support [file-url]
          - update boot-loader file-url
config
    - system
        - security
            - tech-support
                - ts-location file-url
                - no ts-location
```

6.13.1.2.2 High availability (redundancy) commands

```
root
- admin
          - redundancy
              - force-switchover [now]
              - rollback-sync
              - synchronize {boot-env | config}
config
    - redundancy
```

© 2024 Nokia.   278

Use subject to Terms available at: www.nokia.com/terms.

```
                  - bgp-evpn-multi-homing     (refer to the "EVPN Command Reference" section in
 the 7705 SAR Services Guide)
              - [no] cert-sync
              - multi-chassis
                    - peer ip-address [create]
                    - no peer ip-address
                        - authentication-key [authentication-key | hash-key] [hash | hash2]
                        - no authentication-key
                        - description description-string
                        - [no] description
                        - [no] mc-firewall
                            - boot-timer interval
                            - no boot-timer
                            - [no] encryption
                                - active-outbound-sa active-outbound-sa
                                - no active-outbound-sa
                                - authen-algorithm authen-algorithm
                                - no authen-algorithm
                                - encryp-algorithm encryp-algorithm
                                - no encryp-algorithm
                                - security-association spi spi authentication-key authentication-key
 encryption-key encryption-key [hash | hash2]
                                - no security-association spi spi
                        - hold-on-neighbor-failure  multiplier
                        - no hold-on-neighbor-failure
                        - keep-alive-interval  interval
                        - no keep-alive-interval
                        - [no] shutdown
                        - system-priority value
                        - no system-priority
                    - [no] mc-lag
                        - hold-on-neighbor-failure multiplier
                        - no hold-on-neighbor-failure
                        - keep-alive-interval interval
                        - no keep-alive-interval
                        - lag lag-id lacp-key admin-key system-id system-id [remote-lag lag-id]
 system-priority system-priority
                        - no lag lag-id
                        - [no] shutdown
                    - [no] shutdown
                    - source-address ip-address
                    - no source-address
          - [no] rollback-sync
          - synchronize {boot-env | config}
config
- system
          - switchover-exec file-url
          - no switchover-exec
```

6.13.1.3 Show commands

```
show
- chassis  [detail]
    - chassis  [environment] [power-feed]
    - redundancy
          - bgp-evpn-multi-homing      (refer to the "EVPN Command Reference" section in
 the 7705 SAR Services Guide)
          - multi-chassis
              - all
              - mc-firewall peer ip-address
              - mc-firewall peer ip-address statistics
```

```
                    - mc-firewall statistics
                    - mc-lag  peer ip-address [lag lag-id]
                    - mc-lag  [peer ip-address [lag lag-id]] statistics
              - synchronization
    - system
              - connections [address ip-address] [port port-number] [detail]
              - cpu [sample-period seconds]
              - cron
                    - schedule [schedule-name] [owner owner-name]
              - dhcp6
              - fp
                    - options
              - information
              - lldp neighbor
              - load-balancing-alg [detail]
              - memory-pools
              - ntp [{peers | peer peer-address} | {servers | server server-address} | [all]]
  [detail]
              - poe
              - ptp
                    - clock clock-id bmc
                    - clock clock-id detail
                    - clock clock-id standby
                    - clock clock-id statistics
                    - clock clock-id summary
                    - clock clock-id unicast
                    - clock clock-id port [port-id [detail]]
                    - clock clock-id ptp-port port-id
                        - peer peer-id [detail]
              - ptp timestamp-stats
              - rollback [rescue]
              - script-control
                    - script [script-name] [owner script-owner]
                    - script-policy policy-name [owner policy-owner]
                    - script-policy run-history [run-state]
              - sntp
              - sync-if-timing
              - thresholds
              - time [detail]
    - time
        - uptime
```

6.13.1.4 Clear commands

```
clear
- screen
    - system
        - ptp
            - clock clock-id statistics
            - clock csm port port-id statistics
        - script-control
            - script-policy
                - completed [policy-name] [owner policy-owner]
        - sync-if-timing {external | ref 1| ref2}
    - trace log
```

6.13.1.5 Debug commands

```
debug
- sync-if-timing
        - force-reference {external | ref1 | ref2}
        - no force-reference
    - [no] system
        - http-connections [host-ip-address/mask]
        - no http-connections
        - ntp [router router-name] [interface ip-int-name]
        - no ntp
    - lag [lag-id lag-id [port port-id]] [all]
    - lag [lag-id lag-id [port port-id]] [sm] [pkt] [cfg] [red] [iom-upd] [port-state] [timers]
[sel-logic] [mc] [mc-pkt]
    - no lag [lag-id lag-id]
```

6.13.2 Command descriptions

- Configuration commands
- Administration commands
- Show commands
- Clear Commands
- Debug Commands

6.13.2.1 Configuration commands

- Generic commands
- System information and general commands
- System alarm commands
- Persistence commands
- System time commands
- CRON commands
- Script control commands
- System synchronization configuration commands
- LLDP system commands
- System PTP commands

6.13.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>redundancy>multi-chassis>peer

config>redundancy>multi-chassis>peer>mc-firewall

config>redundancy>multi-chassis>peer>mc-lag

config>system>cron>schedule

config>system>fp>options>vpls-high-scale

config>system>lldp

config>system>ptp>clock

config>system>ptp>clock>port

config>system>ptp>clock>ptp-port

config>system>script-control>script

config>system>script-control>script-policy

config>system>sync-if-timing>bits>input

config>system>sync-if-timing>bits>output

config>system>sync-if-timing>external

config>system>sync-if-timing>ref1

config>system>sync-if-timing>ref2

config>system>time>ntp

config>system>time>sntp

Description

This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Default

no shutdown

description

Syntax

description *description-string*

no description

Context

config>redundancy>multi-chassis>peer

config>system>cron>schedule

config>system>persistence>dhcp-server

config>system>ptp>clock>alternate-profile

config>system>ptp>clock>ptp-port>peer

config>system>script-control>script

Description

This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default

n/a — no description is associated with the configuration context

Parameters

description-string

the description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (such as #, $, and spaces), the entire string must be enclosed within double quotes.

6.13.2.1.2 System information and general commands

atm

Syntax

atm

Context

config>system

Description

This command enables the context to configure system-wide ATM parameters.

atm-location-id

Syntax

atm-location-id *location-id*

no atm-location-id

Context

config>system>atm

Description

This command indicates the location ID for ATM OAM.

See the 7705 SAR Quality of Service Guide, "ATM QoS Traffic Descriptor Profiles", for information about ATM QoS policies and the 7705 SAR Services Guide, "VLL Services" for information about ATM-related service parameters.

Default

no atm-location-id

Parameters

location-id

specifies the 16 octets that identifies the system loopback location ID as required by the ATM OAM Loopback capability. This textual convention is defined in ITU-T standard I.610.

Invalid values include a location ID where the first octet is: 00, FF, 6A

Acceptable location-ids include values where the first octet is: 01, 03

Other values are not accepted.

Values   01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

boot-bad-exec

Syntax

boot-bad-exec *file-url*

no boot-bad-exec

Context

config>system

Description

Use this command to configure a URL for a CLI script to execute following a failure of a boot-up configuration. The command specifies a URL for the CLI scripts to be run following the completion of the boot-up configuration. A URL must be specified or no action is taken.

The commands are persistent between router (re)boots and are included in the configuration saves **(admin>save)**.

Also see the related command exec.

Default

no boot-bad-exec

Parameters

file-url

specifies the location and name of the CLI script file executed following failure of the boot-up configuration file execution. When this parameter is not specified, no CLI script file is executed. (See Table 14: URL types and syntax for parameter descriptions.)

boot-good-exec

Syntax

boot-good-exec *file-url*

no boot-good-exec

Context

config>system

Description

Use this command to configure a URL for a CLI script to execute following the success of a boot-up configuration.

Also see the related command exec.

Default

no boot-good-exec

Parameters

file-url

specifies the location and name of the CLI script file executed following successful completion of the boot-up configuration file execution. When this parameter is not specified, no CLI script file is executed. (See Table 14: URL types and syntax for parameter descriptions.)

clli-code

Syntax

clli-code *clli-code*

no clli-code

Context

config>system

Description

This command creates a Common Language Location Identifier (CLLI) code string for the 7705 SAR. A CLLI code is an 11-character standardized geographic identifier that uniquely identifies geographic locations and certain functional categories of equipment unique to the telecommunications industry.

No CLLI validity checks other than truncating or padding the string to 11 characters are performed.

Only one CLLI code can be configured. If multiple CLLI codes are configured, the last one entered overwrites the previous entry.

The **no** form of the command removes the CLLI code.

Default

n/a — no CLLI codes are configured

Parameters

clli-code

the 11-character string CLLI code. Any printable, 7-bit ASCII characters can be used within the string. If the string contains spaces, the entire string must be enclosed within double

quotes. If more than 11 characters are entered, the string is truncated. If fewer than 11 characters are entered, the string is padded with spaces.

config-backup

Syntax

config-backup *count*

no config-backup

Context

config>system

Description

This command configures the maximum number of backup versions maintained for configuration files and BOF.

For example, if the **config-backup** *count* is set to 5 and the configuration file is called `xyz.cfg`, the file `xyz.cfg` is saved with a .1 extension when the **save** command is executed. Each subsequent **config-backup** command increments the numeric extension until the maximum count is reached.

- xyz.cfg
- xyz.cfg.1
- xyz.cfg.2
- xyz.cfg.3
- xyz.cfg.4
- xyz.cfg.5
- xyz.ndx

Each persistent index file is updated at the same time as the associated configuration file. When the index file is updated, then the save is performed to `xyz.cfg` and the index file is created as `xyz.ndx`. Synchronization between the active and standby CSM is performed for all configurations and their associated persistent index files.

The **no** form of the command returns the configuration to the default value.

Default

5

Parameters

count

the maximum number of backup revisions

Values   1 to 9

contact

Syntax

contact *contact-name*

no contact

Context

config>system

Description

This command creates a text string that identifies the contact name for the device.

Only one contact can be configured. If multiple contacts are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default.

Default

n/a — no contact name is configured

Parameters

contact-name

the contact name character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains spaces, the entire string must be enclosed within double quotes.

coordinates

Syntax

coordinates *coordinates*

no coordinates

Context

config>system

Description

This command creates a text string that identifies the system coordinates for the device location. For example, the command **coordinates** "37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.

Only one set of coordinates can be configured. If multiple coordinates are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default

n/a — no coordinates are configured

Parameters

coordinates

the coordinates describing the device location character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains spaces, the entire string must be enclosed within double quotes. If the coordinates are subsequently used by an algorithm that locates the exact position of this node, then the string must match the requirements of the algorithm.

fp

Syntax

fp

Context

config>system

Description

This command enters the context to issue forwarding path commands.

Default

n/a

options

Syntax

options

Context

config>system>fp

Description

This command enters the context to configure forwarding path options.

Default

n/a

vpls-high-scale

Syntax

vpls-high-scale

Context

config>system>fp>options

Description

This command enters the context to enable or disable VPLS scalability with the **shutdown** command.

VPLS scalability is only supported on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18. VPLS scalability cannot be enabled if any of the following are configured in the system:

- access or network IP interfaces (GRT/IES/VPRN) on a 16-port T1/E1 ASAP Adapter card, version 2, 32-port T1/E1 ASAP Adapter card, 4-port OC3/STM1 Clear Channel Adapter card, 2-port OC3/STM1 Channelized Adapter card, or 4-port DS3/E3 Adapter card.

- VPLS residential ATM SAPs

VPLS high-scale limits are supported on access and network links on the following cards:

- 2-port 10GigE (Ethernet) Adapter card
- 8-port Gigabit Ethernet Adapter card
- 10-port 1GigE/1-port 10GigE X-Adapter card
- Packet Microwave Adapter card
- 4-port OC3/STM1 / 1-port OC12/STM4 Adapter card

By default, VPLS scalability is disabled and the 7705 SAR-8 Shelf V2 and 7705 SAR-18 support only 64 VPLS instances. You can enable up to 255 VPLS instances by issuing the **no shutdown** command under this context.

After the **no shutdown** command is issued, the Admin state for **vpls-high-scale** is enabled but the Oper state remains disabled and you cannot create more than 64 VPLS instances. You must issue an **admin save** command and reboot the node for the configuration change to take effect.

To disable VPLS scalability, you must lower the number of VPLS services to 64 or fewer before issuing the **shutdown** command under this context. The VPLS service ID numbers are not relevant, as long as the maximum number of services is 64. You must issue an **admin save** command and reboot the node for the configuration change to take effect.

Default

n/a

identifier

Syntax

[**no**] **identifier** *id*

Context

config>system

Description

This command configures a static system identifier for the 7705 SAR. The system identifier can be used to uniquely identify the 7705 SAR in the network instead of the system IP address, as a system IP address can change dynamically using DHCP when the 7705 SAR is acting as a DHCP client and the DHCP server-facing interface is unnumbered. To prevent management systems (for example, the NSP NFM-P) from rediscovering a node based on a system IP address that has been changed via DHCP, and therefore losing historical data attributed to a specific system IP address, a static system identifier should be configured.

The system identifier takes the form of an IPv4 address. This address is not advertised in IGP or BGP and is used solely as a node identifier.

The **no** form of the command deletes the system identifier.

Default

no identifier

Parameters

id

configures an IPv4 address to be used as the system identifier

Values   any valid IPv4 address

load-balancing

Syntax

load-balancing

Context

config>system

Description

This command enables the context to configure load balancing parameters.

l4-load-balancing

Syntax

[**no**] **l4-load-balancing**

Context

config>system>load-balancing

Description

This command configures system-wide Layer 4 load balancing. The configuration at the system level can enable or disable load balancing across all IP interfaces. When enabled, Layer 4 source and destination port fields of incoming TCP/UDP packets are included in the hashing calculation to randomly determine the distribution of packets. Adding the Layer 4 source and destination port fields to the hashing algorithm generates a higher degree of randomness and a more even distribution of packets across the available ECMP paths or LAG ports.

Default

no l4-load-balancing

lsr-load-balancing

Syntax

lsr-load-balancing *hashing-algorithm* [**bottom-of-stack** *hashing-treatment*][**use-ingress-port**]

no lsr-load-balancing

Context

config>system>load-balancing

Description

This command configures system-wide LSR load balancing. Hashing can be enabled on the IP header at an LSR to send labeled packets over multiple equal-cost paths in an LDP LSP and/or over multiple links of a LAG group in all types of LSPs.

The **bottom-of-stack** option determines the significance of the bottom-of-stack label (VC label) based on which label stack profile option is specified.

When LSR load balancing is enabled, the default configuration for the hashing algorithm is label-only (**lbl-only**) hashing, and the default configuration for the bottom-of-stack hashing treatment is **profile-1**.

The **use-ingress-port** option, when enabled, specifies that the ingress port are used by the hashing algorithm at the LSR. This option should be enabled for ingress LAG ports because packets with the same label stack can arrive on all ports of a LAG interface. In this case, using the ingress port in the hashing algorithm results in better egress load balancing, especially for pseudowires.

The option should be disabled for LDP ECMP so that the ingress port is not used by the hashing algorithm. For ingress LDP ECMP, if the ingress port is used by the hashing algorithm, the hash distribution could be biased, especially for pseudowires.

LSR load-balancing configuration on an interface overrides the system-wide LSR load-balancing settings for the interface.

Default

no lsr-load-balancing

Parameters

hashing-algorithm

specifies the hashing algorithm

Values

lbl-only	hashing is done on the MPLS label stack, up to a maximum of 10 labels
lbl-ip	hashing is done on the MPLS label stack and the IPv4 source and destination IP address if an IPv4 header is present after the MPLS labels
lbl-ip-l4-teid	hashing is done on the MPLS label stack, the IPv4 source and destination IP address (if present), then on the Layer 4 source and destination UDP or TCP port fields (if present) and the TEID in the GTP header (if present)

Default   lbl-only

hashing-treatment

specifies which label stack profile option to use; profiles determine the significance of the bottom-of-stack label (VC label)

Values

profile-1	favors better load balancing for pseudowires when the VC label distribution is contiguous
profile-2	similar to profile-1 where the VC labels are contiguous, but provides an alternate distribution
profile-3	all labels have equal influence in hash key generation

Default   profile-1

use-ingress-port

when configured, specifies that the ingress port is used by the hashing algorithm at the LSR

system-ip-load-balancing

Syntax

[**no**] **system-ip-load-balancing**

Context

config>system>load-balancing

Description

This command enables the use of the system IP address in the hash algorithm to add a per-system variable. This can help to guard against cases where multiple routers, in series, ends up hashing traffic to the same ECMP or LAG path. The algorithm based on the system IP address is included by default.

Default

system-ip-load-balancing

location

Syntax

location *location*

no location

Context

config>system

Description

This command creates a text string that identifies the system location for the device.

Only one location can be configured. If multiple locations are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default

n/a — no system location is configured

Parameters

location

the location as a character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains spaces, the entire string must be enclosed within double quotes.

name

Syntax

name *system-name*

no name

Context

config>system

Description

This command creates a system name string for the device.

For example, system-name parameter ALU-1 for the **name** command configures the device name as ALU-1.

```
ABC>config>system# name ALU-1
ALU-1>config>system#
```

Only one system name can be configured. If multiple system names are configured, the last one encountered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default

The default system name is set to the chassis serial number which is read from the backplane EEPROM.

Parameters

system-name

> the system name as a character string. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains spaces, the entire string must be enclosed within double quotes.

power-feed-monitoring

Syntax

[no] **power-feed-monitoring {A | B | C}**

Context

config>system

Description

This command suppresses power feed monitoring and alarms on the secondary input power feed of a chassis when that power feed is not in use. Use this command when monitoring and raising alarms on the unused power input is not required. Suppressing monitoring and alarms on an unused input power feed results in the following:

- logging of input power feed failures is suppressed

- any alarms that have been raised on an unused power feed are cleared when the **no power-feed-monitoring** command is applied to that power feed

- in the Power Feed Information output of the **show>chassis** command, the status of the unused input power feed appears as "not monitored"

- for chassis that use the Status LED to indicate alarms, the Status LED is lit green if no other alarm conditions exist; for chassis that have alarm LEDs, the critical alarm LED is unlit if no other critical alarm conditions exist. For the 7705 SAR-Hc, the alarm LED is unlit if no other alarm condition exists.

Power feed monitoring and alarming is enabled by default.

Default

power-feed-monitoring

Parameters

- **A** - corresponds to the first input power feed
- **B** - corresponds to the second input power feed
- **C** - corresponds to the AC power input on the high-voltage chassis variant of the 7705 SAR-H

6.13.2.1.3 System alarm commands

thresholds

Syntax

thresholds

Context

config>system

Description

This command enables the context to configure monitoring thresholds.

cflash-cap-alarm

Syntax

cflash-cap-alarm *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]

no cflash-cap-alarm *cflash-id*

Context

config>system>thresholds

Description

This command enables capacity monitoring of the compact flash specified in this command. The severity level is Alarm. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold alarm.

Parameters

cflash-id

the *cflash-id* specifies the name of the cflash device to be monitored (see Table 14: URL types and syntax for parameter descriptions and values)

rising-threshold *threshold*

> specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is greater than or equal to this threshold and the associated *startup-alarm* is equal to *rising* or *either*.

> After a rising threshold crossing event is generated, another such event is not generated until the sampled value falls below this threshold and reaches less than or equal to the *falling-threshold* value.

> The threshold values represent units of 512 bytes.

> > **Values**   -2147483648 to 2147483647

> > **Default**   0

falling-threshold *threshold*

> specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is less than or equal to this threshold and the associated *startup-alarm* is equal to *falling* or *either*.

> After a falling threshold crossing event is generated, another such event is not generated until the sampled value rises above this threshold and reaches greater than or equal to the *rising-threshold* value.

> The threshold values represent units of 512 bytes.

> > **Values**   -2147483648 to 2147483647

> > **Default**   0

seconds

> specifies the polling period, in seconds, over which the data is sampled and compared with the rising and falling thresholds

> > **Values**   1 to 2147483647

rmon-event-type

> specifies the type of notification action to be taken when this event occurs

> > **Values**   **log** — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

> > > **trap** — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, Telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

> > > **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated

none — no action is taken

> **Default**   both

alarm-type

specifies the alarm that may be sent when this alarm is first created

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

> **Values**   **rising, falling, either**

> **Default**   either

Configuration example:

```
cflash-cap-alarm cf1-A: rising-threshold 50000000 falling-
threshold 49999900 interval 120 rmon-event-type both start-alarm rising
```

cflash-cap-warn

Syntax

cflash-cap-warn *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]

no cflash-cap-warn *cflash-id*

Context

config>system>thresholds

Description

This command enables capacity monitoring of the compact flash specified in this command. The severity level is Warning. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold warning.

Parameters

cflash-id

the *cflash-id* specifies the name of the cflash device to be monitored (see Table 14: URL types and syntax for parameter descriptions and values)

rising-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event is not generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold values represent units of 512 bytes.

> **Values**   -2147483648 to 2147483647

> **Default**   0

falling-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event is not generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold values represent units of 512 bytes.

> **Values**   -2147483648 to 2147483647

> **Default**   0

seconds

specifies the polling period over which the data is sampled and compared with the rising and falling thresholds

> **Values**   1 to 2147483647

rmon-event-type

specifies the type of notification action to be taken when this event occurs

> **Values**   **log** — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.
>
> **trap** — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, Telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.
>
> **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated
>
> **none** — no action is taken

> **Default**   both

alarm-type

specifies the alarm that may be sent when this alarm is first created

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values   **rising, falling, either**

Default   either

Configuration example:

```
cflash-cap-warn cf1-B: rising-threshold 2000000 falling-
threshold 1999900 interval 240 rmon-event-type trap start-alarm either
```

memory-use-alarm

Syntax

memory-use-alarm rising-threshold *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]

no memory-use-alarm

Context

config>system>thresholds

Description

The memory thresholds are based on monitoring the TIMETRA-SYSTEM-MIB sgiMemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Alarm.

The **absolute** sample type method is used.

The **no** form of this command removes the configured memory threshold alarm.

Parameters

rising-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event is not generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold values are in bytes.

Values   -2147483648 to 2147483647

Default   0

falling-threshold *threshold*

        specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

        After a falling threshold crossing event is generated, another such event is not generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

        The threshold values are in bytes.

            Values   -2147483648 to 2147483647

            Default   0

seconds

        specifies the polling period over which the data is sampled and compared with the rising and falling thresholds

            Values   1 to 2147483647

rmon-event-type

        specifies the type of notification action to be taken when this event occurs

            Values   **log** — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the CLI command.

                            trap — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, Telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

                            both — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated

                            none — no action is taken

            Default   both

alarm-type

        specifies the alarm that may be sent when this alarm is first created

        If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

        If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

            Values   **rising, falling, either**

            Default   either

Configuration example:

```
memory-use-alarm rising-threshold 50000000 falling-threshold 45999999 interval
 500
rmon-event-type both start-alarm either
```

memory-use-warn

Syntax

memory-use-warn rising-threshold *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]

no memory-use-warn

Context

config>system>thresholds

Description

The memory thresholds are based on monitoring the TIMETRA-SYSTEM-MIB sgiMemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Warning.

The **absolute** sample type method is used.

The **no** form of this command removes the configured compact flash threshold warning.

Parameters

rising-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event is not generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold values are in bytes.

      Values   -2147483648 to 2147483647

      Default   0

falling-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event is not generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold values are in bytes.

> **Values**   -2147483648 to 2147483647

> **Default**   0

seconds

specifies the polling period over which the data is sampled and compared with the rising and falling thresholds

> **Values**   1 to 2147483647

rmon-event-type

specifies the type of notification action to be taken when this event occurs

> **Values**   **log** — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.
>
> **trap** — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, Telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.
>
> **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated
>
> **none** — no action is taken

> **Default**   both

alarm-type

specifies the alarm that may be sent when this alarm is first created

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

> **Values**   **rising, falling, either**

> **Default**   either

Configuration example:

```
memory-use-warn rising-threshold 500000 falling-threshold 400000 interval 800
  rmon-
event-type log start-alarm falling
```

rmon

Syntax

rmon

Context

config>system>thresholds

Description

This command enables the context to configure generic RMON alarms and events.

Generic RMON alarms can be created on any SNMP object-ID that is valid for RMON monitoring (for example, an integer-based datatype).

The configuration of an **event** controls the generation and notification of threshold crossing events configured with the **alarm** command.

alarm

Syntax

alarm *rmon-alarm-id* **variable-oid** *oid-string* **interval** *seconds* [*sample-type*] [**startup-alarm** *alarm-type*] [**rising-event** *rmon-event-id* **rising-threshold** *threshold*] [**falling-event** *rmon-event-id* **falling threshold** *threshold*] [**owner** *owner-string*]

no alarm *rmon-alarm-id*

Context

config>system>thresholds>rmon

Description

The **alarm** command configures an entry in the RMON-MIB alarm table. The **alarm** command controls the monitoring and triggering of threshold crossing events. In order for notification or logging of a threshold crossing event to occur, there must be at least one associated **rmon>event** configured.

The agent periodically takes statistical sample values from the MIB variable specified for monitoring and compares them to thresholds that have been configured with the **alarm** command. The **alarm** command configures the MIB variable to be monitored, the polling period (interval), sampling type (absolute or delta value), and rising and falling threshold parameters. If a sample has crossed a threshold value, the associated event is generated.

Use the **no** form of this command to remove an *rmon-alarm-id* from the configuration.

Parameters

rmon-alarm-id

a numerical identifier for the alarm being configured. The number of alarms that can be created is limited to 1200.

Values   1 to 65535

Default   n/a

oid-string

the SNMP object identifier of the particular variable to be sampled. Only SNMP variables that resolve to an ASN.1 primitive type of integer (integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. The *oid-string* may be expressed using either the dotted string notation or as object name plus dotted instance identifier. For example, "1.3.6.1.2.1.2.2.1.10.184582144" or "ifInOctets.184582144".

The *oid-string* has a maximum length of 255 characters.

Default   n/a

seconds

the interval in seconds specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. When setting this interval value, care should be taken in the case of "delta" type sampling – the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2147483647 – 1 during a single sampling interval. Care should also be taken not to set the interval value too low to avoid creating unnecessary processing overhead.

Values   1 to 2147483647

Default   n/a

sample-type

specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds

Values   **absolute** — specifies that the value of the selected variable is compared directly with the thresholds at the end of the sampling interval

delta — specifies that the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds

Default   absolute

alarm-type

specifies the alarm that may be sent when this alarm is first created

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values   **rising, falling, either**

Default   either

rising-event *rmon-event-id*

the identifier of the **rmon>event** that specifies the action to be taken when a rising threshold crossing event occurs

If there is no corresponding event configured for the specified *rmon-event-id*, then no association exists and no action is taken.

If the *rmon-event-id* has a value of zero (0), no associated event exists.

If an *rmon-event-id* is configured, the CLI requires a **rising-threshold** to also be configured.

> **Values** 0 to 65535

> **Default** 0

rising-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event is not generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

> **Values** -2147483648 to 2147483647

> **Default** 0

falling-event *rmon-event-id*

the identifier of the **rmon>event** that specifies the action to be taken when a falling threshold crossing event occurs

If there is no corresponding event configured for the specified *rmon-event-id*, then no association exists and no action is taken.

If the *rmon-event-id* has a value of zero (0), no associated event exists.

If an *rmon-event-id* is configured, the CLI requires a **falling-threshold** to also be configured.

> **Values** -2147483648 to 2147483647

> **Default** 0

falling-threshold *threshold*

specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event is generated. A single threshold crossing event is also generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event is not generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

Values   -2147483648 to 2147483647

Default   0

owner-string

the creator of this alarm, a string up to 80 characters in length. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarm table by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner is not normally configured by CLI users.

Default   TiMOS CLI

Configuration example:

```
alarm 3 variable-oid ifInOctets.184582144 interval 20 sample-
type delta start-alarm
either rising-event 5 rising-threshold 10000 falling-event 5
 falling-threshold 9000
owner "TiMOS CLI"
```

event

Syntax

event *rmon-event-id* [*event-type*] [**description** *description-string*] [**owner** *owner-string*]

no event *rmon-event-id*

Context

config>system>thresholds>rmon

Description

This command configures an entry in the RMON-MIB event table. The command controls the generation and notification of threshold crossing events configured with the **alarm** command. When a threshold crossing event is triggered, the **rmon>event** configuration optionally specifies if an entry in the RMON-MIB log table should be created to record the occurrence of the event. It may also specify that an SNMP notification (trap) should be generated for the event. The RMON-MIB defines two notifications for threshold crossing events: Rising Alarm and Falling Alarm.

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the TiMOS event logs. However, when the *event-type* is set to **trap**, the generation of a Rising Alarm or Falling Alarm notification creates an entry in the TiMOS event logs and that is distributed to whatever TiMOS log destinations are configured: CONSOLE, session, memory, file, syslog, or SNMP trap destination.

The TiMOS logger message includes a rising or falling threshold crossing event indicator, the sample type (absolute or delta), the sampled value, the threshold value, the *rmon-alarm-id*, the associated *rmon-event-id*, and the sampled SNMP object identifier.

Use the **no** form of this command to remove an *rmon-event-id* from the configuration.

Parameters

rmon-event-id

the identifier of the RMON event

> **Values**   0 to 65535

> **Default**   0

event-type

specifies the type of notification action to be taken

> **Values**   **log** — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.
>
> **trap** — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, Telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.
>
> **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated
>
> **none** — no action is taken

> **Default**   both

description-string

a user-configurable string, up to 80 characters in length, that can be used to identify the purpose of this event. If the string contains special characters (such as #, $, and spaces), the entire string must be enclosed within double quotes.

> **Default**   n/a

owner-string

the creator of this alarm, a string up to 80 characters in length. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarm table by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner is not normally configured by CLI users.

> **Default**   TiMOS CLI

Configuration example:

```
event 5 rmon-event-type both description "alarm testing" owner "TiMOS CLI"
```

6.13.2.1.4 Persistence commands

persistence

Syntax

persistence

Context

config>system

Description

This command enables the context to configure persistence parameters on the system.

The persistence feature allows lease information about DHCP servers to be kept across reboots. This information can include data such as the IP address, MAC binding information, and lease length information.

Default

n/a

dhcp-server

Syntax

dhcp-server

Context

config>system>persistence

Description

This command configures DHCP server persistence parameters.

location

Syntax

location *cflash-id*

no location

Context

config>system>persistence>dhcp-server

Description

This command instructs the system where to write the file. The name of the file is dhcp-serv.001. On boot-up, the system scans the file systems looking for dhcp-serv.001. If the system finds the file, it loads it.

The **no** form of this command returns the system to the default.

Default

no location

Parameters

cflash-id

the location of the compact flash device. On all 7705 SAR systems except the 7705 SAR-18, the location is cf3:. On the 7705 SAR-18, the location is cf1:, cf2:, or cf3:.

6.13.2.1.5 System time commands

set-time

Syntax

set-time [*date*] [*time*]

Context

admin

Description

This command sets the local system time.

The time entered should be accurate for the time zone configured for the system. The system converts the local time to UTC before saving to the system clock, which is always set to UTC. This command does not take into account any daylight saving offset if defined.

Parameters

date

the local date and time accurate to the minute in the YYYY/MM/DD format

Values   *YYYY* is the 4-digit year

MM is the 2-digit month

DD is the 2-digit date

time

the time (accurate to the second) in the *hh*:*mm*[:*ss*] format. If no seconds value is entered, the seconds are reset to :00.

Values   *hh* is the 2-digit hour in 24 hour format (00=midnight, 12=noon)

mm is the 2-digit minute

Default   0

time

Syntax

time

Context

config>system

Description

This command enables the context to configure the system time zone and time synchronization parameters.

dst-zone

Syntax

[**no**] **dst-zone** [*std-zone-name* | *non-std-zone-name*]

Context

config>system>time

Description

This command configures the start and end dates and offset for summer time or daylight savings time to override system defaults or for user defined time zones.

When configured, the time is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.

If the time zone configured is listed in Table 23: System-defined time zones , then the starting and ending parameters and offset do not need to be configured with this command unless it is necessary to override the system defaults. The command returns an error if the start and ending dates and times are not available either in Table 23: System-defined time zones or entered as optional parameters in this command.

Up to five summer time zones may be configured; for example, for five successive years or for five different time zones. Configuring a sixth entry returns an error message. If no summer (daylight savings) time is supplied, it is assumed no summer time adjustment is required.

The **no** form of the command removes a configured summer (daylight savings) time entry.

Default

n/a — no summer time is configured

Parameters

std-zone-name

the standard time zone name. The standard name must be a system-defined zone in Table 23: System-defined time zones . For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining *start-date*,

end-date and *offset* parameters need to be provided unless it is necessary to override the system defaults for the time zone.

> **Values**   std-zone-name ADT, AKDT, CDT, CEST, EDT, EEST, MDT, PDT, WEST

non-std-zone-name

the non-standard time zone name. Create a user-defined name using the zone command.

> **Values**   5 characters maximum

end

Syntax

end *end-week end-day end-month hours-minutes*

Context

config>system>time>dst-zone

Description

This command configures the end of summer time settings.

Parameters

end-week

specifies the starting week of the month when the summer time ends

> **Values**   first, second, third, fourth, last

> **Default**   first

end-day

specifies the starting day of the week when the summer time ends

> **Values**   sunday, monday, tuesday, wednesday, thursday, friday, saturday

> **Default**   sunday

end-month

specifies the starting month of the year when the summer time ends

> **Values**   january, february, march, april, may, june, july, august, september, october, november, december}

> **Default**   january

hours

specifies the hour at which the summer time ends

> **Values**   0 to 24

Default   0

minutes

specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time ends

Values   0 to 59

Default   0

offset

Syntax

offset *offset*

Context

config>system>time>dst-zone

Description

This command specifies the number of minutes that is added to the time when summer time takes effect. The same number of minutes are subtracted from the time when the summer time ends.

Parameters

offset

the number of minutes added to the time at the beginning of summer time and subtracted at the end of summer time, expressed as an integer

Values   0 to 60

Default   60

start

Syntax

start *start-week start-day start-month hours-minutes*

Context

config>system>time>dst-zone

Description

This command configures start of summer time settings.

Parameters

start-week

specifies the starting week of the month when the summer time takes effect

Values   first, second, third, fourth, last

Default   first

start-day

specifies the starting day of the week when the summer time takes effect

Values   sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default   sunday

start-month

the starting month of the year when the summer time takes effect

Values   january, february, march, april, may, june, july, august, september, october, november, december

Default   january

hours

specifies the hour at which the summer time takes effect

Default   0

minutes

specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time takes effect

Default   0

gnss

Syntax

gnss

Context

config>system>time

Description

This command enables the context to create or modify **gnss** parameters for time.

Default

n/a

port

Syntax

port *port-id* **time-ref-priority** *priority-value*

no port

Context

config>system>time>gnss

Description

This command specifies a GNSS receiver port as a synchronous timing source. The specific GNSS receiver port is identified by *port-id* and has an assigned *priority-value*.

Default

no port

Parameters

port-id

identifies the GNSS receiver port in the *slot/mda/port* format

priority-value

specifies the priority order of the specified GNSS receiver port configured as the time reference. The lower the number, the higher the priority. GNSS should be granted the highest priority whenever available.

Values   1 to 16

ntp

Syntax

[**no**] **ntp**

Context

config>system>time

Description

This command enables the context to configure Network Time Protocol (NTP) and its operation. This protocol defines a method to accurately distribute and maintain time for network elements. Furthermore, this capability allows for the synchronization of clocks between the various network elements. The **no** form of the command stops the execution of NTP and removes its configuration.

Default

n/a

authentication-check

Syntax

[**no**] **authentication-check**

Context

config>system>time>ntp

Description

This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key ID, type, or key values.

When authentication is configured, NTP PDUs received on an interface or the management port are authenticated on receipt and rejected if there is a mismatch in the authentication key ID, type, or key value.

When **authentication-check** is enabled, NTP PDUs are authenticated on receipt and rejected if there is a mismatch in the authentication key ID, type, or key value. Any mismatches cause a counter to be incremented: one counter for type, one for key ID, and one for key value mismatches. These counters are visible in the **show>system>ntp** command output.

The **no** form of this command allows mismatched packets to be accepted (overriding authentication); however, the counters are maintained.

Default

authentication-check

authentication-key

Syntax

authentication-key *key-id* **key** *key* [**hash** | **hash2**] **type** {**des** | **message-digest**}

no authentication-key *key-id*

Context

config>system>time>ntp

Description

This command sets the authentication key ID, type, and key value used to authenticate NTP PDUs sent to or received from other network elements participating in the NTP protocol. For authentication to work, the authentication key ID, type, and key value must match.

Configuring the **authentication-key** with a *key-id* value that matches an existing key overrides the existing entry.

Recipients of the NTP packets must have the same authentication key ID, type, and key value to use the data transmitted by this node.

The **no** form of the command removes the authentication key.

Default

n/a

Parameters

key-id

the authentication key identifier used by the node when transmitting or receiving NTP packets

Values   1 to 255

key

the authentication key associated with the configured key ID. The configured value is the actual value used by other network elements to authenticate the NTP packet.

Values   any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

hash

specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2

specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone. This means that the **hash2** encrypted key cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

type

the authentication type, either DES or message-digest

Values   **des** — specifies that DES authentication is used for this key. The **des** value is not supported in FIPS-140-2 mode.

message-digest — specifies that MD5 authentication in accordance with RFC 2104 is used for this key

broadcast

Syntax

broadcast [**router** *router-name*] {**interface** *ip-int-name*} [**key-id** *key-id*] [**version** *version*] [**ttl** *ttl*]

no broadcast [**router** *router-name*] {**interface** *ip-int-name*}

Context

config>system>time>ntp

Description

This command configures the node to transmit NTP broadcast packets on the specified interface. Because broadcast messages can easily be spoofed, authentication is strongly recommended.

Broadcast server capability can also be enabled on an interface within a VPRN context. See the 7705 SAR Services Guide, "VPRN NTP Commands", for information.

The **no** form of this command removes the interface from the configuration.

Default

n/a

Parameters

router-name

the name of the router used to transmit NTP packets. Select management to use the Management port (Ethernet port on the CSM).

Values   Base | management

Default   Base

ip-int-name

the local interface on which to transmit NTP broadcast packets. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Values   32 character maximum

key-id

identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets from and to an NTP server and peers. If an NTP packet is received by this node, both the authentication key and authentication type must be valid; otherwise, the packet is rejected and an event or trap is generated. When this parameter is omitted from the configuration, packets are sent unencrypted.

Values   1 to 255

version

the NTP version number that this node generates. This parameter does not need to be configured when the node is in NTP client mode because all versions are accepted.

Values   2 to 4

Default   4

ttl

the IP Time To Live (TTL) value

Values   1 to 255

broadcastclient

Syntax

broadcastclient [**router** *router-name*] {**interface** *ip-int-name*} [**authenticate**]

no broadcastclient [**router** *router-name*] {**interface** *ip-int-name*}

Context

config>system>time>ntp

Description

This command configures an interface to receive NTP broadcast packets on a particular subnet. Because broadcast messages can easily be spoofed, authentication is strongly recommended. If **broadcastclient** is not configured, received NTP broadcast traffic is ignored. Use the **show>system>ntp** command to view the state of the configuration.

When the **authenticate** parameter is specified, the received authentication *key-id* must have been configured with the **authentication-key** command, and the key ID type and key value must also match.

The **no** form of this command removes the interface from the configuration.

Default

n/a

Parameters

router-name

> the name of the router used to receive NTP packets. Select management to use the Management port (Ethernet port on the CSM)

>> **Values**   Base | management

>> **Default**   Base

ip-int-name

> the local interface on which to receive NTP broadcast packets. If the string contains special characters (such as #, $, and spaces), the entire string must be enclosed within double quotes.

>> **Values**   32 character maximum

authenticate

> specifies that authentication is required. If authentication is required, the authentication *key-id* received in a message must have been configured with the **authentication-key** command, and the key ID type and key value must match.

mda-timestamp

Syntax

[**no**] **mda-timestamp**

Context

config>system>time>ntp

Description

This command enables more accurate timestamping for in-band NTP packets. When enabled, timestamping is performed on an adapter card by the network processor as packets ingress and egress the router. This reduces packet delay variability.

The **mda-timestamp** command can only be set if NTP is shut down and the NTP servers are not associated with an authentication key. The command is only supported on Ethernet-based adapter cards. Enabling this command does not change the behavior of NTP over the Management port.

The **no** form of this command returns the system to its default behavior of having NTP packets timestamped by the CSM.

Default

no mda-timestamp

multicast

Syntax

multicast [**key-id** *key-id*] [**version** *version*]

no multicast

Context

config>system>time>ntp

Description

This command configures the node to transmit NTP multicast packets on the Management port. Because multicast messages can easily be spoofed, authentication is strongly recommended.

The **no** form of this command disables transmission of multicast packets on the Management port.

Default

n/a

Parameters

key-id

the authentication key ID used by the node to transmit NTP multicast packets. When this parameter is omitted from the configuration, packets are sent unencrypted.

Values   1 to 255

version

the NTP version number that is generated by the node. When the node is in NTP client mode, this parameter does not need to be configured because all versions are accepted.

Values   2 to 4

Default   4

multicastclient

Syntax

multicastclient [**authenticate**]

no multicastclient

Context

config>system>time>ntp

Description

This command configures the node to receive NTP multicast messages on the Management port. If **multicastclient** is not configured, received NTP multicast traffic is ignored. Use the **show>system>ntp** command to view the state of the configuration.

When the **authenticate** parameter is specified, the received authentication *key-id* must have been configured with the **authentication-key** command, and the key ID type and key value must also match.

The **no** form of this command disables the receipt of multicast messages on the Management port.

Default

n/a

Parameters

authenticate

specifies that authentication is required. If authentication is required, the authentication *key-id* received in a message must have been configured with the **authentication-key** command, and the key ID type and key value must match.

ntp-server

Syntax

ntp-server [**authenticate**]

no ntp-server

Context

config>system>time>ntp

Description

This command configures the node to assume the role of an NTP server. Unless the **ntp-server** command is used, the node functions as an NTP client only and does not distribute time to downstream network elements.

Default

no ntp-server

Parameters

authenticate

specifies that authentication is required. If authentication is required, the authentication *key-id* received in a message must have been configured with the **authentication-key** command, and the key ID, type, and key values must match. The authentication key from the received messages is used for the transmitted messages.

peer

Syntax

peer *ip-address* [**key-id** *key-id*] [**version** *version*] [**prefer**]

no peer *ip-address*

Context

config>system>time>ntp

Description

This command configures symmetric active mode for an NTP peer. It is recommended that only known time servers be configured as peers and that authentication be enabled.

Successful authentication requires that both peers have the same authentication key ID, type, and key values. The key ID identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP peer. When an NTP packet is received by a peer, if the authentication key ID, type, and key values do not match, the packet is rejected and an event or trap is generated.

When configuring more than one peer, one remote system can be configured as the preferred peer. If a second peer is configured as preferred, the new entry overrides the old entry.

The **no** form of the command removes the specified peer.

Default

n/a

Parameters

ip-address

the IP address of the peer that requires a peering relationship to be set up. The address can be IPv4 or IPv6.

key-id

the authentication key ID

> **Values**   1 to 255

version

the NTP version number that is generated by the node. When the node is in NTP client mode, this parameter does not need to be configured because all versions are accepted.

> **Values**   2 to 4

> **Default**   4

prefer

specifies the configured peer as the preferred peer

server

Syntax

server {*ip-address* | **system-time**} [**key-id** *key-id*] [**version** *version*] [**prefer**]

no server {*ip-address* | **system-time**}

Context

config>system>time>ntp

Description

This command specifies the source that is to be used as an NTP server. The source can be specified with an IPv4 address, an IPv6 address, or the **system-time** keyword.

The NTP clock in the 7705 SAR can recover time from a local PTP or GNSS source. This is achieved by configuring the PTP clock or GNSS receiver as the internal system time. The internal system time can then be identified as the preferred source of NTP timing into the network with the **system-time** and **prefer** parameters. After PTP or GNSS has established a UTC traceable time, it is always the source for time into NTP even if the system time goes into time holdover for any reason. When the internal PTP clock or GNSS is identified as the server for NTP, NTP promotes the internal NTP server (the 7705 SAR) to Stratum-1 level, which may affect the NTP network topology.

Up to five NTP servers can be configured. When configuring more than one server, one remote system can be configured as the preferred server. If a second server is configured as preferred, the new entry overrides the old entry.

The **no** form of this command removes the specified NTP server from the configuration.

Default

n/a

Parameters

ip-address

the IP address of the node to be used as the NTP server to this network element

system-time

specifies that the internal system time configured with PTP or GNSS is the time server into the NTP process. The **prefer** parameter is mandatory with this option.

version

the NTP version number that is expected by this node

Values 2 to 4

Default 4

key-id

the identifier for the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP server. If an NTP packet is received by this node, the authentication key ID, type, and key values must be valid; otherwise, the packet is rejected and an event or trap is generated.

Values 1 to 255

prefer

specifies the configured source as the preferred source that is to be used as an NTP server

ptp

Syntax

ptp

Context

config>system>time

Description

This command enables the context to create or modify **ptp** parameters for time.

clock

Syntax

clock *clock-id* **time-ref-priority** *priority-value*

clock csm time-ref-priority *priority-value*

no clock

Context

config>system>time>ptp

Description

This command specifies the PTP (Precision Time Protocol) source as an option for recovered time for the 1pps (1 pulse per second) port. The specific PTP clock is identified by *clock-id* and has an assigned *priority-value*.

Default

no clock

Parameters

clock-id

specifies which configured clock is being used as the time reference

Values 1 to 16

priority-value

specifies the priority order of the specified clock configured as the time reference

Values 1 to 16

csm

keyword to specify the CSM as the time reference

sntp

Syntax

[**no**] **sntp**

Context

config>system>time

Description

This command enables the context to edit the Simple Network Time Protocol (SNTP).

SNTP can be configured in either broadcast or unicast client mode. SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from SNTP/NTP servers. It cannot be used to provide time services to other systems.

The system clock is automatically adjusted at system initialization time or when the protocol first starts up.

When the time differential between the SNTP/NTP server and the system is more than 2.5 seconds, the time on the system is gradually adjusted.

SNTP is created in an administratively enabled state (**no shutdown**).

The **no** form of the command removes the SNTP instance and configuration. SNTP does not need to be administratively disabled when removing the SNTP instance and configuration.

Default

no sntp

broadcast-client

Syntax

[**no**] **broadcast-client**

Context

config>system>time>sntp

Description

This command enables listening to SNTP/NTP broadcast messages on interfaces with broadcast client enabled at global device level.

When this global parameter is configured, then the **ntp-broadcast** parameter must be configured on selected interfaces on which NTP broadcasts are transmitted.

SNTP must be shut down before changing either to or from broadcast mode.

The **no** form of the command disables broadcast client mode.

Default

no broadcast-client

server-address

Syntax

server-address *ip-address* [**version** *version-number*] [**normal** | **preferred**]

[**interval** *seconds*]

no server-address *ip-address*

Context

config>system>time>sntp

Description

This command creates an SNTP server for unicast client mode.

Parameters

ip-address

specifies the IP address of the SNTP server

version-number

specifies the SNTP version supported by this server

             Values   1 to 3

            Default   3

normal | preferred

> specifies the preference value for this SNTP server. When more than one time-server is configured, one server can have preference over others. The value for that server should be set to **preferred**. Only one server in the table can be a preferred server.

            Default   normal

seconds

> specifies the frequency at which this server is queried

            Values   64 to 1024

            Default   64

tod-1pps

Syntax

tod-1pps

Context

config>system>time

Description

This command enables the context to create or modify **tod-1pps** connector parameters.

message-type

Syntax

message-type {ct | cm | irig-b002-b122 | irig-b003-b123 | irig-b006-b126 | irig-b007-b127}

no message-type

Context

config>system>time>tod-1pps

Description

This command specifies the format for the Time of Day message that is transmitted out the time of day (ToD) or ToD/PPS Out port on the following:

- 7705 SAR-M
- 7705 SAR-H

- 7705 SAR-A
- 7705 SAR-Ax
- 7705 SAR-X

On the 7705 SAR-H, the Time of Day message output is only available when the router is configured with an active IP PTP timeReceiver clock or boundary clock. For all other routers, the Time of Day message output is available when the router is configured with an active IP PTP timeReceiver clock or boundary clock or when Time of Day is recovered from an Ethernet PTP clock or integrated GNSS.

Default

no message-type

Parameters

ct

China Telecom; not available on the 7705 SAR-H

cm

China Mobile; not available on the 7705 SAR-H

irig-b002-b122 | irig-b003-b123 | irig-b006-b126 | irig-b007-b127

specifies IRIG-B message format; available on the 7705 SAR-H only

output

Syntax

[**no**] **output**

Context

config>system>time>tod-1pps

Description

This command specifies whether the 1pps output is enabled. When disabled, neither the 1pps nor the RS-422 serial port is available.

Default

no output

zone

Syntax

zone {*std-zone-name* | *non-std-zone-name*} [*hh* [*:mm*]]

no zone

Context

config>system>time

Description

This command sets the time zone and/or time zone offset for the device.

The 7705 SAR supports system-defined and user-defined time zones. The system-defined time zones are listed in Table 23: System-defined time zones .

For user-defined time zones, the zone and the UTC offset must be specified.

The **no** form of the command reverts to the default of Coordinated Universal Time (UTC). If the time zone in use was a user-defined time zone, the time zone is deleted. If a dst-zone command has been configured that references the zone, the summer commands must be deleted before the zone can be reset to UTC.

Default

zone utc - the time zone is set for Coordinated Universal Time (UTC)

Parameters

std-zone-name

the standard time zone name. The standard name must be a system-defined zone in Table 23: System-defined time zones . For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining *start-date*, *end-date* and *offset* parameters need to be provided unless it is necessary to override the system defaults for the time zone.

For system-defined time zones, a different offset cannot be specified. If a new time zone is needed with a different offset, the user must create a new time zone. Some system-defined time zones have implicit summer time settings that causes the switchover to summer time to occur automatically; in this case, configuring the dst-zone parameter is not required.

A user-defined time zone name is case-sensitive and can be up to 5 characters in length.

    Values   A user-defined value can be up to 5 characters or one of the following values:

        GMT, BST, IST, WET, WEST, CET, CEST, EET, EEST, MSK, MSD, AST, ADT, EST, EDT, ET, CST, CDT, CT, MST, MDT, MT, PST, PDT, PT, HST, AKST, AKDT, WAST, CAST, EAST

non-std-zone-name

the non-standard time zone name

    Values   Up to 5 characters maximum

hh [:mm]

the hours and minutes offset from UTC time, expressed as integers. Some time zones do not have an offset that is an integral number of hours. In these instances, the *minutes-offset* must be specified. For example, the time zone in Pirlanngimpi, Australia is UTC + 9.5 hours.

    Values   hours: -11 to 11

                minutes: 0 to 59

Default   hours: 0

minutes: 0

6.13.2.1.6 CRON commands

cron

Syntax

cron

Context

config>system

Description

This command enables the context to configure periodic and date- and time-based scheduling.

CRON can be used, for example, to schedule Service Assurance Agent (SAA) functions. CRON functions include the ability to specify scripts that need to be run and when they are scheduled. Reboots, peer turn-ups, and SAA tests can be scheduled with CRON, as well as OAM events such as connectivity checks or troubleshooting runs.

schedule

Syntax

[**no**] **schedule** *schedule-name* [**owner** *schedule-owner*]

Context

config>system>cron

Description

This command configures a schedule name and optional schedule owner.

Default

no schedule

Parameters

schedule-name

the name of the schedule, up to 32 characters in length

schedule-owner

the name of the owner, up to 32 characters in length. The owner name is an arbitrary string; it is not associated with an actual CLI user.

Default   "TiMOS CLI"

count

Syntax

count *number*

no count

Context

config>system>cron>schedule

Description

This command configures the number of times a CRON periodic schedule is run. For example, if the **interval** is set to 600 and the **count** is set to 4, the schedule runs 4 times at 600-second intervals.

Default

no count

Parameters

number

the number of times the schedule is run

Values   1 to 65535

day-of-month

Syntax

day-of-month {*day-number* [*..day-number*] | **all**}

no day-of-month

Context

config>system>cron>schedule

Description

This command specifies on which days of the month the schedule executes. Multiple days of the month can be specified. If multiple days are configured, each of them triggers the schedule. If a **day-of-month** is configured without configuring month, hour, and minute, the schedule does not execute.

Using the **weekday** command as well as the **day-of-month** command may cause the schedule to run twice in a week. For example, if today is Monday, January 1, and month is set to January, **weekday** is set to Tuesday, and **day-of-month** is set to the 5th day of the month, the schedule runs on Tuesday (January 2) and on Friday (January 5).

The **no** form of this command removes the specified **day-of-month** or all **day-of-month** configurations.

Default

no day-of-month

Parameters

day-number

positive integers specify the day of the month beginning on the first of the month. Negative integers specify the day of the month beginning on the last day of the month. For example, configuring **day-of-month -5, 5** in a month that has 31 days specifies the schedule to execute on the 27th and 5th of that month.

Integer values must map to a valid day for the specified month. For example, February 30 is not a valid date.

Values   1 to 31, -31 to -1 (maximum 62 day-numbers)

all

specifies all days of the month

end-time

Syntax

end-time [*date* | *day-name*] *time*

no end-time

Context

config>system>cron>schedule

Description

This command is used concurrently with schedule type **calendar** or **periodic**. If the schedule is configured as **calendar**, the end-time determines on which date the schedule ends. If the schedule is configured as **periodic**, the end-time determines at which interval the schedule ends.

If **no end-time** is specified, the schedule runs indefinitely.

Default

no end-time

Parameters

date

the date that the schedule ends

Values   yyyy/mm/dd in year/month/day number format

day-name

the day of the week that the schedule ends

Values   sunday | monday | tuesday | wednesday | thursday | friday | saturday

time

the time on the configured day that the schedule ends

Values   hh:mm in hour:minute format

hour

Syntax
hour {*..hour-number* [*..hour-number*] | **all**}

no hour

Context
config>system>cron>schedule

Description
This command specifies at which hour the schedule executes. Multiple hours can be specified. If multiple hours are configured, each of them triggers the schedule. If an hour is configured without configuring month, weekday or day-of-month, and minute, the schedule does not execute.

The **no** form of this command removes the specified hour or all configured hours.

Default
no hour

Parameters
hour-number

the hour that the schedule executes

Values   0 to 23 (maximum 24 *hour-numbers*)

all

specifies all hours

interval

Syntax
interval *seconds*

no interval

Context
config>system>cron>schedule

Description
This command specifies the interval between each periodic schedule run.

Default

no interval

Parameters

seconds

the interval, in seconds, between each schedule run

Values   30 to 4294967295

minute

Syntax

minute {*minute-number* [**..**minute-number] | **all**}

no minute

Context

config>system>cron>schedule

Description

This command specifies at which minute the schedule executes. Multiple minutes can be specified. If multiple minutes are configured, each of them triggers the schedule. If a minute is configured without configuring month, weekday or day-of-month, and hour, the schedule does not execute.

The **no** form of this command removes the specified minute or all configured minutes.

Default

no minute

Parameters

minute-number

the minute that the schedule executes

Values   0 to 59 (maximum 60 *minute-numbers*)

all

specifies all minutes

month

Syntax

month {*month-number* [**..**month-number] | *month-name* [**..**month-name] | **all**}

no month

Context

config>system>cron>schedule

Description

This command specifies on which month the schedule executes. Multiple months can be specified. If multiple months are configured, each of them triggers the schedule. If a month is configured without configuring weekday or day-of-month, hour, and minute, the schedule does not execute.

The **no** form of this command removes the specified month or all configured months.

Default

no month

Parameters

month-number

the month that the schedule executes, by number

> **Values**   1 to 12 (maximum 12 *month-numbers*)

month-name

the month that the schedule executes, by name

> **Values**   january, february, march, april, may, june, july, august, september, october, november, december (maximum 12 *month-names*)

all

specifies all months

script-policy

Syntax

script-policy *policy-name* [**owner** *policy-owner*]

no script-policy

Context

config>system>cron>schedule

Description

This command specifies the script policy associated with the script to be run by the CRON schedule. The script policy must have already been created in the **config>system>script-control** context.

Default

no script-policy

Parameters

policy-name

the name of the script policy associated with the needed script

policy-owner

the name of the owner that, combined with the script policy name, is associated with the needed script

type

Syntax

type *schedule-type*

Context

config>system>cron>schedule

Description

This command configures how the schedule runs (periodically, on a specified date or dates, or one time only).

Default

periodic

Parameters

schedule-type

the type of schedule

Values **periodic** — specifies that the schedule runs at a specified interval. The interval value must be configured.

calendar — specifies that the schedule runs based on a calendar. The month, weekday or day-of-month, hour, and minute must be configured.

oneshot — specifies that the schedule runs one time only, then enters a shutdown state. The month, weekday or day-of-month, hour, and minute must be configured.

weekday

Syntax

weekday {*weekday-number* [**..***weekday-number*] | *day-name* [**..***day-name*] | **all**}

no weekday

Context

config>system>cron>schedule

Description

This command specifies on which days of the week the schedule executes. Multiple days of the week can be specified. If multiple days are configured, each of them triggers the schedule. If a weekday is configured without configuring month, hour, and minute, the schedule does not execute.

Using the **weekday** command as well as the **day-of-month** command may cause the schedule to run twice in a week. For example, if today is Monday, January 1, and **month** is set to January, **weekday** is set to Tuesday, and **day-of-month** is set to the 5th day of the month, the schedule runs on Tuesday (January 2) and on Friday (January 5).

The **no** form of this command removes the specified weekday or all configured weekdays.

Default

no weekday

Parameters

weekday-number

the day of the week that the schedule executes, by number

Values　　1 to 7 (maximum 7 *weekday-numbers*)

day-name

the day of the week that the schedule executes, by name

Values　　sunday, monday, tuesday, wednesday, thursday, friday, saturday (maximum 7 *day-names*)

all

specifies all days of the week

6.13.2.1.7 Script control commands

script-control

Syntax

script-control

Context

config>system

Description

This command enables the context to configure CLI script parameters.

script

Syntax

[**no**] **script** *script-name* [**owner** *script-owner*]

Context

config>system>script-control

Description

This command assigns a name and optional owner to a script text file that contains a list of CLI commands to be executed. The owner is an arbitrary string; it is not associated with an actual CLI user.

Multiple owners can be associated with a script name, and each script name/owner combination is unique.

The scripts are not authorized against the owner but can be configured to execute under a particular user context in order for authorization to be performed. See the 7705 SAR System Management Guide, "CLI Script Authorization Commands", for information.

The **no** form of the command deletes the script name.

Default

no script

Parameters

script-name

the name of the script, up to 32 characters in length

script-owner

the name of the script owner, up to 32 characters in length

Default   "TiMOS CLI"

location

Syntax

location *file-url*

no location

Context

config>system>script-control>script

Description

This command specifies the location of the script text file, either on the local compact flash or on a remote FTP server.

The **no** form of the command removes the location.

Default

no location

Parameters

file-url

the local or remote URL for the file location (see Table 14: URL types and syntax for parameter descriptions)

script-policy

Syntax

[**no**] **script-policy** *policy-name* [**owner** *policy-owner*]

Context

config>system>script-control

Description

This command configures a script policy. The script policy is assigned a name and optional owner. The owner is an arbitrary string; it is not associated with an actual CLI user.

Multiple owners can be associated with a script policy, and each script policy name/owner combination is unique.

A script policy cannot be shut down while a running history exists for that policy. The script policy must be shut down before the script file location can be changed.

Default

no script-policy

Parameters

policy-name

the name of the script policy, up to 32 characters in length

policy-owner

the name of the script policy owner, up to 32 characters in length

Default   "TiMOS CLI"

expire-time

Syntax

expire-time {*seconds* | **forever**}

Context

config>system>script-control>script-policy

Description

This command configures the maximum length of time to keep the run history status entry from a script run.

Default

expire-time 3600

Parameters

seconds

length of time to keep the run history status entry, in seconds

Values   0 to 21474836

forever

specifies to keep the run history status entry indefinitely

lifetime

Syntax

lifetime {*seconds* | **forever**}

Context

config>system>script-control>script-policy

Description

This command configures the maximum length of time that a script may run.

Default

lifetime 3600

Parameters

seconds

the maximum length of time that a script may run, in seconds

Values   0 to 21474836

forever

specifies to allow a script to run indefinitely

max-completed

Syntax

max-completed *unsigned*

Context

config>system>script-control>script-policy

Description

This command specifies the maximum number of script run history status entries to keep.

The system maintains the script run history table, which has a maximum size of 255 entries. Entries are removed from this table when the **max-completed** or **expire-time** thresholds are crossed. If the table reaches the maximum value, no further scripts are run until older run history entries expire (because of the **expire-time** setting), or entries are manually cleared.

Default

max-completed 1

Parameters

unsigned

the maximum number of script run history status entries to keep

Values   1 to 1500

results

Syntax

results *file-url*

no results

Context

config>system>script-control>script-policy

Description

This command specifies the location where the system stores the results of the script run, either on a local compact flash or on an FTP server.

When a script is run, the results are stored in the specified location, and a date and time suffix is added to the filename in the format yyyymmdd-hhmmss.µµµµµµ.out. The microseconds are padded to 6 characters with leading zeros.

The **no** form of the command removes the file location from the configuration. Scripts do not execute if there is no results file location defined.

Default

no results

Parameters

file-url

the local or remote URL for the results file location (see Table 14: URL types and syntax for parameter descriptions)

script

Syntax

script *script-name* [**owner** *script-owner*]

no script

Context

config>system>script-control>script-policy

Description

This command associates the script defined under the **config>system>script-control** context with this script policy.

The **no** form of the command removes the script from the script policy.

Default

no script

Parameters

script-name

the name of the defined script

script-owner

the name of the defined script owner associated with the script name

6.13.2.1.8 System synchronization configuration commands

sync-if-timing

Syntax

sync-if-timing

Context

config>system

Description

This command creates or edits the context to create or modify timing reference parameters.

Default

not enabled (The **ref-order** must be specified in order for this command to be enabled.)

abort

Syntax

abort

Context

config>system>sync-if-timing

Description

This command is required to discard changes that have been made to the synchronous interface timing configuration during a session.

begin

Syntax

begin

Context

config>system>sync-if-timing

Description

This command is required to enter the mode to create or edit the system synchronous interface timing configuration.

bits

Syntax

bits

Context

config>system>sync-if-timing

Description

This command enables the context to configure parameters for BITS timing on the 7705 SAR-18. The BITS input and output ports can be configured for T1/E1 or 2 MHz G.703 signals.

input

Syntax

input

Context

config>system>sync-if-timing>bits

Description

This command enables the context to configure BITS input timing ports parameters on the 7705 SAR-18.

interface-type

Syntax

interface-type {ds1 [{esf | sf}] | e1 [{pcm30crc | pcm31crc}] | 2048khz-G703}

no interface-type

Context

config>system>sync-if-timing>bits

Description

This command specifies the signal type for the BITS input and output ports. If you configure the signal type as **ds1**, the system automatically defaults to **esf**. If you configure the signal type as **e1**, the system automatically defaults to **pcm30crc**.

The **no** form of the command reverts to the default configuration.

Default

ds1 esf

Parameters

ds1 esf

specifies Extended Super Frame (ESF). ESF is a framing type used on DS1 circuits. ESF consists of 24 192-bit frames. The 193rd bit provides timing and other functions.

ds1 sf

specifies Super Frame (SF), also called D4 framing. SF is a common framing type used on DS1 circuits. SF consists of 12 192-bit frames. The 193rd bit provides error checking and other functions. ESF supersedes SF.

e1 pcm30crc

specifies PCM30CRC as the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with Cyclic Redundancy Check (CRC) protection.

e1 pcm31crc

specifies PCM31CRC as the PCM type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.

output

Syntax

output

Context

config>system>sync-if-timing>bits

Description

This command enables the context to configure BITS output port parameters on the 7705 SAR-18.

line-length

Syntax

line-length {**110** | **220** | **330** | **440** | **550** | **660**}

Context

config>system>sync-if-timing>bits>output

Description

This command configures the line length, in feet, between the network element and the central clock (BITS/SSU).

This command is only applicable when the interface-type is DS1.

Default

110

Parameters

110

specifies a line length from 0 to 110 ft

220

specifies a line length from 111 to 220 ft

330

specifies a line length from 221 to 330 ft

440

specifies a line length from 331 to 440 ft

550

specifies a line length from 441 to 550 ft

660

specifies a line length from 551 to 660 ft

source

Syntax

source {line-ref | internal-clock}

Context

config>system>sync-if-timing>bits>output

Description

This command configures the source of the BITS output ports in the 7705 SAR-18.

By default the source is configured as **internal-clock**, which provides a filtered signal from the output of the node's central clock. The central clock output is usually used when no BITS/SASE device is present. When an external BITS/SASE clock is present, it is often desirable to provide an unfiltered clock reference to it by configuring **line-ref**. When the **line-ref** parameter is configured, the recovered clock from ref1 or ref2 (based on configuration of the **ref-order** and **ql-selection** commands) is transmitted directly out the BITS output port without filtering.

Default

internal-clock

Parameters

line-ref

> BITS output timing is selected from one of the input references, without any filtering

internal-clock

> BITS output timing is driven from the node's central clock (filtered)

ql-override

Syntax

ql-override {prs | stu | st2 | tnc | st3e | st3 | smc | prc | ssu-a | ssu-b | sec | eec1 | eec2}

no ql-override

Context

config>system>sync-if-timing>external

config>system>sync-if-timing>bits

config>system>sync-if-timing>ref1

config>system>sync-if-timing>ref2

Description

This command configures a static quality level value. This value overrides any dynamic quality level value received by the Synchronization Status Messaging (SSM) process.

Default

no ql-override (for external timing references, ql-override stu is equivalent to no ql-override)

Parameters

prs

SONET Primary Reference Source Traceable

stu

SONET Synchronous Traceability Unknown

st2

SONET Stratum 2 Traceable

tnc

SONET Transit Node Clock Traceable

st3e

SONET Stratum 3E Traceable

st3

SONET Stratum 3 Traceable

smc

SONET Minimum Clock Traceable

prc

SDH Primary Reference Clock Traceable

ssu-a

SDH Primary Level Synchronization Supply Unit Traceable

ssu-b

SDH Second Level Synchronization Supply Unit Traceable

sec

SDH Synchronous Equipment Clock Traceable

eec1

Ethernet Equipment Clock Option 1 Traceable (SDH)

eec2

Ethernet Equipment Clock Option 2 Traceable (SONET)

ssm-bit

Syntax

ssm-bit *sa-bit*

Context

config>system>sync-if-timing>bits

Description

This command configures which Sa-bit to use for conveying Synchronization Status Messaging (SSM) information when the interface type is E1.

Default

Sa8

Parameters

sa-bit

specifies the Sa-bit value

Values   Sa4 to Sa8

commit

Syntax

commit

Context

config>system>sync-if-timing

Description

This command is required to save the changes made to the system synchronous interface timing configuration.

external

Syntax

external

Context

config>system>sync-if-timing

Description

This command enables the context to configure parameters for external timing via the port on the CSM. This can be used to reference external synchronization signals.

input-interface

Syntax

input-interface

Context

config>system>sync-if-timing>external

Description

This command enables the context to configure parameters for external input timing interface via the port on the CSM.

impedance

Syntax

impedance {**high-impedance** | **50-Ohm** | **75-Ohm**}

Context

config>system>sync-if-timing>external>input-interface

Description

This command configures the impedance of the external input timing port. The command is only applicable to the 7705 SAR-8 Shelf V2, 7705 SAR-H, and 7705 SAR-M.

Default

50-Ohm

Parameters

high-impedance

specifies a high input impedance value

50-Ohm

specifies a 50 Ω input impedance value

75-Ohm

specifies a 75 Ω input impedance value

type

Syntax

type {**2048khz-G703** | **5mhz** | **10mhz**}

no type

Context

config>system>sync-if-timing>external>input-interface

config>system>sync-if-timing>external>output-interface

Description

This command configures the interface type of the external timing port.

The **no** form of the command reverts to the default.

Default

2048 kHz-G703

Parameters

2048khz-G703

specifies a G703 2048 kHz clock

5mhz

specifies a 5 MHz sine clock

10mhz

specifies a 10 MHz sine clock

output-interface

Syntax

output-interface

Context

config>system>sync-if-timing>external

Description

This command enables the context to configure parameters for external output timing interface via the port on the CSM.

Default

n/a

ql-selection

Syntax

[**no**] **ql-selection**

Context

config>system>sync-if-timing

Description

This command enables SSM encoding as a means of timing reference selection.

Default

no ql-selection

ref-order

Syntax

ref-order *first second* [*third*]

no ref-order

Context

config>system>sync-if-timing

Description

The synchronous equipment timing source can lock to three different timing reference inputs, those specified in the ref1, ref2, external, and bits command configuration. This command organizes the priority order of the timing references.

If a reference source is disabled, then the clock from the next reference source as defined by **ref-order** is used. If the reference sources are disabled, then clocking is derived from a local oscillator.

If a **sync-if-timing** reference is linked to a source port that is operationally down, the port is no longer qualified as a valid reference.

For unfiltered BITS output (T4), all reference sources are valid options, except the BITS input, which is excluded to avoid a timing loop. Because the same priority order is used for the SETG output (T0), the BITS input option must be set as the first (highest-priority) reference option.

The **no** form of the command resets the reference order to the default values.

Default

external, ref1 ref2

Parameters

first

specifies the first timing reference to use in the reference order sequence

Values   ref1, ref2, external, bits

second

specifies the second timing reference to use in the reference order sequence

Values   ref1, ref2, external, bits

third

specifies the third timing reference to use in the reference order sequence

Values   ref1, ref2, external, bits

ref1

Syntax

ref1

Context

config>system>sync-if-timing

Description

This command enables the context to configure parameters for the first timing reference.

ref2

Syntax

ref2

Context

config>system>sync-if-timing

Description

This command enables the context to configure parameters for the second timing reference.

source-port

Syntax

source-port *port-id* [**adaptive**]

no source-port

Context

config>system>sync-if-timing>ref1

config>system>sync-if-timing>ref2

Description

This command configures the source port for timing reference **ref1** or **ref2**.

The timing reference can either be timing extracted from the receive port (line-timed) or packetized data of a TDM PW (adaptive). If the adaptive option is not selected, the system uses line timing mode. If the line timing is from a port that becomes unavailable or the link goes down, then the reference sources are re-evaluated according to the reference order configured by the ref-order command.

Line timing is supported on T1/E1 ports of the 7705 SAR-M and 7705 SAR-A and on the T1/E1 ports of the 7705 SAR-H 4-port T1/E1 and RS-232 Combination module.

Line timing is also supported in the form of synchronous Ethernet on all RJ45 and optical SFP Ethernet ports on the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-Wx, 7705 SAR-X, and 7705 SAR-Ax. The 7705 SAR-A supports line timing on its synchronous Ethernet-capable ports (1 to 8) when they are fixed RJ45 or optical SFP.

In addition, line timing is supported on the following modules:

- 2-port 10GigE (Ethernet) module

- 6-port SAR-M Ethernet module

- 4-port SAR-H Fast Ethernet module

On the 7705 SAR-8 Shelf V2 or 7705 SAR-18, line timing is supported on:

- T1/E1 ports on the 16-port T1/E1 ASAP Adapter card and 32-port T1/E1 ASAP Adapter card

- Ethernet SFP ports with SFPs that support synchronous Ethernet on the 6-port Ethernet 10Gbps Adapter card, 8-port Gigabit Ethernet Adapter card, Packet Microwave Adapter card, 2-port 10GigE (Ethernet) Adapter card, and 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only)

- SONET/SDH ports on the 4-port OC3/STM1 Clear Channel Adapter card and 2-port OC3/STM1 Channelized Adapter card

- DS3/E3 ports on the 4-port DS3/E3 Adapter card

Adaptive timing is supported on the T1/E1 ports on the 7705 SAR-X, 7705 SAR-M, and 7705 SAR-A. On the 7705 SAR-8 Shelf V2 and 7705 SAR-18, adaptive timing is supported on the 16-port T1/E1 ASAP Adapter card and the 32-port T1/E1 ASAP Adapter card configured with one or more TDM PWs. Adaptive timing is also supported on the T1/E1 ports of the 4-port T1/E1 and RS-232 Combination module.

> **Note:** The PW terminated on channel group 1 is used to extract the ACR timing.

Synchronous Ethernet ports can supply a timing reference on the 7705 SAR-M, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, and 7705 SAR-X. Two T1/E1 ports can supply a timing reference on the 7705 SAR-X and on the 7705 SAR-M and 7705 SAR-A (variants with T1/E1 ports).

On the 7705 SAR-H and 7705 SAR-Hc, all RJ45 Ethernet ports and SFP ports support synchronous Ethernet and can supply a timing reference to be used as a source of node synchronization. When the 4-port T1/E1 and RS-232 Combination module is installed in the 7705 SAR-H, a single T1/E1 port on the module can supply a timing reference.

When the 2-port 10GigE (Ethernet) module or 6-port SAR-M Ethernet module is installed in the 7705 SAR-M, the ports on the module can supply a timing reference.

The 7705 SAR-8 Shelf V2 and 7705 SAR-18 can receive one or two timing references depending on the port and card type supplying the reference. A timing reference can come from:

- a single SONET/SDH port on the 4-port OC3/STM1 Clear Channel Adapter card

- two DS3/E3 ports on the 4-port DS3/E3 Adapter card

- two SONET/SDH ports on the 2-port OC3/STM1 Channelized Adapter card

- two synchronous Ethernet ports on the 6-port Ethernet 10Gbps Adapter card, 8-port Gigabit Ethernet Adapter card, 10-port 1GigE/1-port 10GigE X-Adapter card (supported on the 7705 SAR-18 only), or 2-port 10GigE (Ethernet) Adapter card

- two T1/E1 ports on the 16-port T1/E1 ASAP Adapter card or 32-port T1/E1 ASAP Adapter card. References must be from different framers; the framers each have eight ports and are grouped as ports 1 to 8, 9 to 16, 17 to 24, and 25 to 32.

- two ports on the Packet Microwave Adapter card: on port 1 or 2, it could be a synchronous Ethernet or PCR-enabled port; on port 3 or 4, it could be a synchronous Ethernet (optical SFP only) or PCR-enabled port (copper-based SFP only); on ports 5 through 8, it could be a synchronous Ethernet (optical SFP only) port.

The **no** form of this command deletes the source port from the reference. An example of when the **no** form would be used is if the user wants to change the reference to a source IP interface to enable PTP. In this case, the user would first delete the PTP using the **no source-port** command, then configure the source IP interface using the source-ptp-clock command.

Parameters

port-id

identifies the port in the slot/mda/port format

adaptive

clock recovery is adaptive, instead of line-timed

source-ptp-clock

Syntax

source-ptp-clock *clock-id*

no source-ptp-clock

Context

config>system>sync-if-timing>ref1

config>system>sync-if-timing>ref2

Description

This command configures the reference source clock using the clock ID configured by the PTP clock command.

Default

no source-ptp-clock

Parameters

clock-id

identifies the PTP clock to use as the reference source clock

Values   1 to 16

revert

Syntax

[**no**] **revert**

Context

config>system>sync-if-timing

Description

This command allows the clock to revert to a higher-priority reference if the current reference goes offline or becomes unstable. With revertive switching enabled, the highest-priority valid timing reference is used. If a reference with a higher priority becomes valid, a reference switchover to that reference is initiated. If a failure on the current reference occurs, the next highest reference takes over. With non-revertive switching, the active reference always remains selected while it is valid, even if a higher-priority reference becomes available. If this reference becomes invalid, a reference switchover to a valid reference with the highest priority is initiated. When the failed reference becomes operational, it is eligible for selection.

Default

no revert

6.13.2.1.9 LLDP system commands

See the *7705 SAR Interface Configuration Guide*, "7705 SAR Interfaces", for LLDP Ethernet port commands.

lldp

Syntax

lldp

Context

config>system

Description

This command enables the context to configure system-wide Link Layer Discovery Protocol (LLDP) parameters.

message-fast-tx

Syntax

message-fast-tx *time*

no message-fast-tx

Context

config>system>lldp

Description

This command configures the interval between LLDPDU transmissions by the LLDP agent during a fast transmission period.

The fast transmission period begins when a new neighbor is detected. During the fast transmission period, LLDPDUs are transmitted at shorter intervals than the standard tx-interval to ensure that more than one LLDPDU is sent to the new neighbor. The first transmission occurs as soon as the new neighbor is detected. The length of the fast transmission period is determined by the number of LLDPDU transmissions (configured by the message-fast-tx-init command) and the interval between them.

The **no** form of the command reverts to the default value.

Default

1

Parameters

time

specifies the interval between LLDPDU transmissions in seconds

Values   1 to 3600

message-fast-tx-init

Syntax

message-fast-tx-init *count*

no message-fast-tx-init

Context

config>system>lldp

Description

This command configures the number of LLDPDUs to send during a fast transmission period.

The fast transmission period begins when a new neighbor is detected. During the fast transmission period, LLDPDUs are transmitted at shorter intervals than the standard tx-interval to ensure that more than one LLDPDU is sent to the new neighbor. The first transmission occurs as soon as the new neighbor is detected. The length of the fast transmission period is determined by the number of LLDPDU transmissions and the interval between them (configured by the message-fast-tx command).

The **no** form of the command reverts to the default value.

Default

4

Parameters

count

specifies the number of LLDPDUs to send during the fast transmission period

Values   1 to 8

notification-interval

Syntax

notification-interval *time*

no notification-interval

Context

config>system>lldp

Description

This command configures the minimum time between change notifications. A change notification is a trap message sent to SNMP whenever a change occurs in the database of LLDP information.

The **no** form of the command reverts to the default value.

Default

5

Parameters

time

specifies the minimum time, in seconds, between change notifications

Values   5 to 3600

reinit-delay

Syntax

reinit-delay time

no reinit-delay

Context

config>system>lldp

Description

This command configures the time before reinitializing LLDP on a port.

The **no** form of the command reverts to the default value.

Default

2

Parameters

time

specifies the time, in seconds, before reinitializing LLDP on a port

Values   1 to 10

tx-credit-max

Syntax

tx-credit-max *count*

no tx-credit-max

Context

config>system>lldp

Description

This command configures the maximum number of consecutive LLDPDUs that can be transmitted at any time.

The **no** form of the command reverts to the default value.

Default

5

Parameters

count

specifies the maximum number of consecutive LLDPDUs transmitted

Values   1 to 100

tx-hold-multiplier

Syntax

tx-hold-multiplier *multiplier*

no tx-hold-multiplier

Context

config>system>lldp

Description

This command configures the multiplier of the transmit interval defined by the tx-interval command.

The transmit interval time multiplied by the **tx-hold-multiplier** is the TTL value in the LLDPDU. The TTL value determines the amount of time the receiving device retains LLDP packet information in local information databases before discarding it.

The **no** form of the command reverts to the default value.

Default

4

Parameters

multiplier

> specifies the multiplier of the transmit interval

> > **Values** 2 to 10

tx-interval

Syntax

tx-interval *interval*

no tx-interval

Context

config>system>lldp

Description

This command configures the LLDP transmit interval time.

The **no** form of the command reverts to the default value.

Default

30

Parameters

interval

> specifies the LLDP transmit interval time in seconds

> > **Values** 5 to 32768

6.13.2.1.10 System PTP commands

Note: The IEEE 1588 Working Group has introduced the terms timeTransmitter and timeReceiver as alternatives to the former master/slave terminology. This section uses the terms **master** and **slave** only when referring to the CLI commands.

ptp

Syntax

ptp

Context

config>system

Description

This command enables the context to create or modify PTP timing parameters.

clock

Syntax

clock *clock-id* [**create**]

no clock

Context

config>system>ptp

Description

This command creates a PTP clock, which can be set to a master (timeTransmitter), slave (timeReceiver), boundary, or transparent clock using the clock-type command. The *clock-id* can be a numeric value (1 to 16) or it can be the keyword csm.

Use the numeric value for PTP clocks that transmit and receive PTP messages using IPv4 or IPv6 encapsulation. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, and 7705 SAR-X, only one PTP instance can be master (timeTransmitter), slave (timeReceiver), or boundary.

Use the **csm** keyword when the PTP clock transmits and receives PTP messages using Ethernet encapsulation. Ethernet-encapsulated PTP messages are processed on the CSM module or CSM functional block.

The **no** form of the command deletes a PTP clock when the *clock-id* is set to a numeric value. The CSM PTP clock cannot be removed.

Parameters

clock-id

specifies the clock ID of this PTP instance

Values   1 to 16 for PTP clocks that use IPv4 or IPv6 encapsulation

csm for the PTP clock that uses Ethernet encapsulation

create

keyword required when first creating the configuration context for a *clock-id* of 1 to 16. When the context is created, you can navigate into the context without the **create** keyword. The **create** keyword is not required when the *clock-id* is **csm**.

alternate-profile

Syntax

alternate-profile *profile-name* [**create**]

no alternate-profile *profile-name*

Context

config>system>ptp>clock

Description

This command configures an alternate profile to be used for PTP messaging. An alternate profile can be used at the edge of a network to provide PTP time or frequency distribution outward to external PTP clocks.

The alternate profile name cannot be "primary" because that is reserved for the primary profile.

The alternate profile cannot be removed if any PTP ports or peers are enabled and using it; the ports or peers must first be shut down.

The **no** form of the command removes the alternate profile configuration.

Default

n/a

Parameters

profile-name

the name of the alternate profile, up to 64 characters

create

keyword required when first creating the alternate profile. When the alternate profile is created, you can navigate into the context without the **create** keyword.

domain

Syntax

domain *domain-value*

no domain

Context

config>system>ptp>clock>alternate-profile

Description

This command defines the PTP device domain as an integer for the alternate profile. A domain consists of one device or multiple PTP devices communicating with each other as defined by the protocol. A PTP domain defines the scope of PTP message communication, state, operations, datasets, and timescale. A domain is configured because it is possible that a deployment could require two PTP instances within a single network element to be programmed with different domain values.

The domain value cannot be changed if any PTP ports or peers are enabled and using the alternate profile.

The **no** form of this command returns the configuration to the default value. The default value varies depending on the configuration of the profile command.

Default

0 when the alternate profile is configured as **iec-61850-9-3-2016**

254 when the alternate profile is configured as **c37dot238-2017**

Parameters

domain-value

specifies the PTP device domain value

Values 0 to 255

initial-time-inaccuracy

Syntax

initial-time-inaccuracy *initial-time-inaccuracy*

no initial-time-inaccuracy

Context

config>system>ptp>clock>alternate-profile

Description

This command sets the time inaccuracy value, representing the total time inaccuracy from the grandmaster clock to the parent clock. This value is added to the mandatory IEEE_C37_238 TLV.

This command is applicable only when the alternate profile is configured as **c37dot238-2017**.

The **no** form of this command returns the configuration to the default value.

Default

0

Parameters

initial-time-inaccuracy

specifies the total inaccuracy on the network in nanoseconds, to be added to the IEEE_C37_238 TLV

>**Values**   0 to 10000000

log-anno-interval

Syntax

log-anno-interval *log-anno-interval*

no log-anno-interval

Context

config>system>ptp>clock>alternate-profile

Description

This command configures the Announce message interval used for multicast messages in the alternate profile. For multicast messages on PTP Ethernet ports, this command configures the message interval used for Announce messages transmitted by the local node. This value has no impact on the interval between executions of the BTCA within the node; that interval is controlled by the *log-anno-interval* value defined for the primary profile.

The **no** form of this command returns the configuration to the default value.

Default

0 (1 packet/s)

Parameters

log-anno-interval

>specifies the expected interval between the reception of Announce messages. This parameter is specified as the logarithm to the base 2, in seconds.

>>**Values**   −3 to 4, where −3 = 0.125 s, −2 = 0.25 s, −1 = 0.5 s, 0 = 1 s, 1 = 2 s, 2 = 4 s, 3 = 8 s, and 4 = 16 s

profile

Syntax

profile {iec-61850-9-3-2016 | c37dot238-2017}

no profile

Context

config>system>ptp>clock>alternate-profile

Description

This command defines the specification rules to be used by the PTP alternate profile. The profile cannot be changed if there are any PTP ports or peers enabled and using the alternate profile; the ports or peers must first be shut down.

The **no** form of this command removes the profile configuration from the alternate profile.

Default

no profile

Parameters

iec-61850-9-3-2016

configures the PTP alternate profile to follow the IEEE 1588-2008 specification rules

c37dot238-2017

configures the PTP alternate profile to follow the C37.238-2017 specification rules

anno-rx-timeout

Syntax

anno-rx-timeout *number-of-timeouts*

no anno-rx-timeout

Context

config>system>ptp>clock

config>system>ptp>clock>ptp-port

Description

This command defines the number of Announce timeouts that need to occur on a PTP timeReceiver port or boundary clock port in timeReceiver mode before communication messages with a timeTransmitter clock are deemed lost and the timeTransmitter clock is considered not available. One timeout in this context is equal to the Announce interval in seconds, calculated using the logarithm 2^log-anno-interval.

The **no** form of this command returns the configuration to the default value.

Default

3

Parameters

number-of-timeouts

specifies the number of timeouts that need to occur before communication messages to a timeTransmitter clock are deemed lost and the timeTransmitter clock is considered not available

Values   2 to 10

apts-asymmetry-compensation

Syntax

[no] apts-asymmetry-compensation

Context

config>system>ptp>clock

Description

This command enables asymmetry compensation mode on the 7705 SAR-8 Shelf V2 or 7705 SAR-18.

The ITU-T G.8275.2 APTS functionality is supported on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18 when equipped with a GNSS Receiver card and two Ethernet adapter cards — one configured as a G.8275.2 timeReceiver clock for backup and one configured as a G.8275.2 boundary clock with timeTransmitter ports.

When GNSS is up, the level of asymmetry on the designated backup timeReceiver clock is monitored when the **apts-asymmetry-compensation** command is enabled. The CSM notes the time and frequency recovery state and the delay asymmetry of the backup timeReceiver clock based on the timestamps exchanged during the last update. If GNSS fails, the measured level of asymmetry is applied to the PTP backup clock to keep time and phase as accurate as possible. The monitored states and values are available via the CLI and SNMP.

This command is only available when the IP PTP *clock-id* parameter value is 1 to 8.

The **no** form of the command removes the APTS asymmetry compensation.

Default

no apts-asymmetry-compensation

clock-mda

Syntax

clock-mda *mda-id*

no clock-mda

Context

config>system>ptp>clock

Description

This command configures the adapter card slot that performs the IEEE 1588v2 clock recovery. On the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, and 7705 SAR-Wx, this slot is always 1/1. On the 7705 SAR-X, this slot is always either 1/2 or 1/3.

This command is only available when the *clock-id* parameter value is 1 to 16.

The **no** form of this command clears the clock recovery adapter card.

Default

n/a

Parameters

mda-id

slot/mda

clock-type

Syntax

clock-type {**ordinary** {**master** | **slave**} | **boundary** | **transparent-e2e**}

no clock-type

Context

config>system>ptp>clock

Description

This command configures the type of clock. The **no** form of the command returns the configuration to the default (**ordinary slave**). The clock type can only be changed when PTP is shut down.

To enable transparent clock processing at the node level, configure a PTP clock with the **transparent-e2e** clock type. The **transparent-e2e** clock type is only available for a PTP clock that transmits and receives PTP messages using IPv4 encapsulation.

Default

ordinary slave

Parameters

ordinary master

configures the clock as an ordinary PTP timeTransmitter

ordinary slave

configures the clock as an ordinary PTP timeReceiver

boundary

configures the clock as a boundary clock capable of functioning as both a timeTransmitter and timeReceiver concurrently

transparent-e2e

configures the clock as a transparent clock. This option is only used for a PTP clock that transmits and receives PTP messages using IPv4 encapsulation, and is only available for the following: 7705 SAR-M, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, and 7705 SAR-X.

domain

Syntax

domain *domain-value*

no domain

Context

config>system>ptp>clock

Description

This command defines the PTP device domain as an integer. A domain consists of one device or multiple PTP devices communicating with each other as defined by the protocol. A PTP domain defines the scope of PTP message communication, state, operations, datasets, and timescale. A domain is configured because it is possible that a deployment could require two PTP instances within a single network element to be programmed with different domain values.

The **no** form of this command returns the configuration to the default value. The default value varies depending on the configuration of the profile command.

Default

0 when the profile is configured as **ieee1588-2008**, **itu-telecom-freq**, or **iec-61850-9-3-2016**

24 when the profile is configured as **g8275dot1-2014**

44 when the profile is configured as **g8275dot2-2016**

254 when the profile is configured as **c37dot238-2017**

Parameters

domain-value

specifies the PTP device domain value

Values   0 to 255

dynamic-peers

Syntax

[**no**] **dynamic-peers**

Context

config>system>ptp>clock

Description

This command allows a timeReceiver clock to connect to the timeTransmitter clock without the timeTransmitter being aware of it. When connected, the timeTransmitter clock or boundary clock assigns the timeReceiver a PTP port or peer ID dynamically.

This command is only available when the *clock-id* parameter value is 1 to 16.

Dynamic peers are not stored in the configuration file. If a timeTransmitter clock with dynamic peers goes down and comes back up, the timeReceiver clocks renegotiate to it and are reassigned resources on the timeTransmitter clock or boundary clock.

The **no** form of this command disables dynamic peers. In this case, the user must manually program any timeReceiver peer clocks into the timeTransmitter clock or boundary clock in order for those clocks to accept those timeReceivers.

Default

no dynamic-peers

freq-source

Syntax

freq-source {**ptp** | **ssu**}

no freq-source

Context

config>system>ptp>clock

Description

This command specifies the administrative frequency source to use for the PTP clock. This selection influences the operational frequency source selected by the system for the PTP clock. If PTP is only used for time of day and the node SSU is being synchronized through a better frequency source externally (for example, through the external timing input port) or through line timing (for example, through a synchronous Ethernet or T1/E1 port), SSU may be configured as the frequency source for the PTP clock. This option allows PTP to use the SSU frequency where available.

This command is only available when the *clock-id* parameter value is 1 to 16.

The **no** form of the command returns the configuration to the default setting.

Default

ptp

Parameters

ptp

configures the PTP clock to use PTP as the frequency source

ssu

configures the PTP clock to use the SSU as the frequency source

local-priority

Syntax

local-priority *priority*

no local-priority

Context

config>system>ptp>clock

config>system>ptp>clock>port

config>system>ptp>clock>ptp-port

Description

This command configures the local priority used to choose between PTP timeTransmitters in the best timeTransmitter clock algorithm (BTCA). If the PTP profile is set to **ieee1588-2008** or **itu-telecom-freq**, this parameter is ignored. The priority of the port or local clock can only be configured if the PTP profile is set to **g8275dot1-2014** or **g8275dot2-2016**. The value of the highest priority is 1 and the value of the lowest priority is 255.

The **no** form of this command returns the configuration to the default value.

Default

128

Parameters

priority

specifies the local priority for choosing the PTP timeTransmitter for the BTCA

Values   1 to 255

log-anno-interval

Syntax

log-anno-interval *log-anno-interval*

no log-anno-interval

Context

config>system>ptp>clock

config>system>ptp>clock>ptp-port

Description

This command configures the Announce message interval used for unicast and multicast messages.

For unicast messages, this command defines the Announce message interval that is requested during unicast negotiation to any peer. This controls the Announce message rate sent from remote peers to the

local node. It does not affect the Announce message rate that may be sent from the local node to remote peers. Remote peers may request an Announce message rate anywhere within the acceptable grant range.

For multicast messages on PTP Ethernet ports, this command configures the message interval used for Announce messages transmitted by the local node.

This value also defines the interval between executions of the BTCA within the node. To minimize BTCA-driven reconfigurations, the IEEE Std 1588-2008 recommends that the Announce message interval be consistent across the entire IEEE 1588 network. The Announce message interval cannot be changed unless PTP is shut down.

The *log-anno-interval* is calculated using the binary logarithm of the value of the interval in seconds before message reception. For example, for an Announce message interval of 8 packets/s (one packet every 0.125 seconds), set this field to log(base2) (0.125) = –3.

The **no** form of this command returns the configuration to the default value. The default value varies depending on the configuration of the profile command.

Default

1 (1 packet every 2 s) when the profile is configured as **ieee1588-2008**

1 (1 packet every 2 s) when the profile is configured as **itu-telecom-freq** for a *clock-id* of 1 to 16 (this profile does not apply when the *clock-id* is **csm**)

–3 (8 packets/s) when the profile is configured as **g8275dot1-2014** or **g8275dot2-2016** (this profile does not apply when the *clock-id* is **csm**)

0 (1 packet/s) when the profile is configured as **iec-61850-9-3-2016** or **c37dot238-2017** and the *clock-id* is **csm** (these profiles do not apply when the *clock-id* is 1 to 16)

Parameters

log-anno-interval

specifies the expected interval between the reception of Announce messages. This parameter is specified as the logarithm to the base 2, in seconds.

Values   –3 to 4, where –3 = 0.125 s, –2 = 0.25 s, –1 = 0.5 s, 0 = 1 s, 1 = 2 s, 2 = 4 s, 3 = 8 s, and 4 = 16 s when the *clock-id* is 1 to 16 (all profiles except for **iec-61850-9-3-2016** and **c37dot238-2017**) or when the *clock-id* is **csm** and the profile is configured as **ieee1588-2008**, **g8275dot1-2014**, **iec-61850-9-3-2016**, or **c37dot238-2017** (the **itu-telecom-freq** and **g8275dot2-2016** profiles do not apply when the *clock-id* is **csm**)

network-type

Syntax

network-type {sdh | sonet}

no network-type

Context

config>system>ptp>clock

Description

This command determines whether to use SDH or SONET values for encoding synchronous status messages. This command only applies to synchronous Ethernet ports and is not configurable on SONET/SDH ports. This command is only available when the *clock-id* parameter is defined as **csm**.

Default

sdh

Parameters

sdh

specifies the values used are as defined in ITU-T G.781 Option 1

sonet

specifies the values used are as defined in ITU-T G.781 Option 2

port

Syntax

port *port-id* [**create**]

no port *port-id*

Context

config>system>ptp>clock

Description

This command configures PTP over Ethernet on the physical port, so that PTP messages are sent and received over the port using Ethernet encapsulation. There are two reserved multicast addresses allocated for PTP messages (see Annex F of IEEE Std 1588- 2008 and the address command). Either address can be configured for the PTP messages sent through this port. The adapter card, module, or fixed platform containing the specified port cannot be deprovisioned while the port is configured for PTP. A port configured for dot1q or qinq encapsulation can be configured as the physical port for PTP over Ethernet. The encapsulation type and the Ethernet port type cannot be changed when PTP Ethernet multicast operation is configured on the port.

This command is only available when the *clock-id* parameter is defined as **csm**.

Default

n/a

Parameters

port-id

specifies the physical port in the format *slot/mda/port*

address

Syntax

address {01:1b:19:00:00:00 | 01:80:c2:00:00:0e}

no address

Context

config>system>ptp>clock>port

Description

This command configures the MAC address to be used as the multicast destination MAC address for transmitted PTP messages. The IEEE Std 1588-2008 Annex F defines the two reserved addresses for PTP messages as:

- 01-1B-19-00-00-00 for all messages except peer delay messages
- 01-80-C2-00-00-0E for peer delay messages

The system accepts PTP messages received using either destination MAC address, regardless of the address configured by this command.

The **no** form of this command returns the address to the default value.

Default

01:1b:19:00:00:00

log-delay-interval

Syntax

log-delay-interval *log-delay-interval*

no log-delay-interval

Context

config>system>ptp>clock>port

Description

This command configures the minimum interval between multicast Delay_Req or PDelay messages for PTP with Ethernet encapsulation. This parameter is applied on a per-port basis and does not apply to peers. PTP timeReceiver ports use this interval unless the parent port indicates a longer interval. PTP timeTransmitter ports advertise this interval to external timeReceiver ports as the minimum acceptable interval for Delay_Req or PDelay messages from those timeReceiver ports. The 7705 SAR supports the IEEE 1588 requirement that a port in timeReceiver mode check the logMessageInterval field of received multicast Delay_Resp or PDelay messages. If the value of the logMessageInterval field for those messages is greater than the value configured locally to generate Delay_Req or PDelay messages, the timeReceiver port must use the longer interval for generating Delay_Req or PDelay messages.

The *log-delay-interval* is calculated using the binary logarithm of the value of the interval in seconds.

The *log-delay-interval* is only applicable when the *clock-id* is **csm**. For PTP with IP encapsulation (*clock-id* is 1 to 16), the value configured for the *log-sync-interval* is also used as the interval for Delay_Req or PDelay messages.

The **no** form of this command returns the configuration to the default value. The default value varies depending on the configuration of the profile command.

Default

–6 when the profile is configured as **ieee1588-2008**

–4 when the profile is configured as **g8275dot1-2014**

0 when the profile is configured as **iec-61850-9-3-2016** or **c37dot238-2017**

Parameters

log-delay-interval

specifies the expected interval between the receipt of Delay_Req or PDelay messages

Values   –6 to 0, where –6 is 64 packets/s, –5 is 32 packets/s, –4 is 16 packets/s, –3 is 8 packets/s, –2 is 4 packets/s, –1 is 2 packets/s, and 0 is 1 packet/s, when the profile is configured as **ieee1588-2008**, **g8275dot1-2014**, **iec-61850-9-3-2016**, or **c37dot238-2017**

log-sync-interval

Syntax

log-sync-interval *log-sync-interval*

no log-sync-interval

Context

config>system>ptp>clock>port

config>system>ptp>clock>ptp-port

Description

This command configures the interval between transmission of synchronization packets for a PTP port in a timeTransmitter state. For PTP with IP encapsulation (*clock-id* is 1 to 16), this value is also used as the interval for Delay_Req messages for this clock.

The **no** form of this command returns the configuration to the default value. The default value varies depending on the configuration of the profile command.

Default

–6 when the profile is configured as **ieee1588-2008**

–6 when the profile is configured as **itu-telecom-freq** for a *clock-id* of 1 to 16 (this profile does not apply when the *clock-id* is **csm**)

–4 when the profile is configured as **g8275dot1-2014** or **g8275dot2-2016** (this profile does not apply when the *clock-id* is **csm**)

0 when the profile is configured as **iec-61850-9-3-2016** or **c37dot238-2017** and the *clock-id* is **csm** (these profiles do not apply when the *clock-id* is 1 to 16)

Parameters

log-sync-interval

specifies the expected interval between the reception of synchronization messages

Values   –7 to –4, where –7 is 128 packets/s, –6 is 64 packets/s, –5 is 32 packets/s, and –4 is 16 packets/s, when the *clock-id* is 1 to 16 (all profiles except for **iec-61850-9-3-2016** and **c37dot238-2017**)

–6 to 0, where –6 is 64 packets/s, –5 is 32 packets/s, –4 is 16 packets/ s, –3 is 8 packets/s, –2 is 4 packets/s, –1 is 2 packets/s, and 0 is 1 packet/s, when the *clock-id* is **csm** and the profile is configured as **ieee1588-2008**, **g8275dot1-2014**, **iec-61850-9-3-2016**, or **c37dot238-2017** (the **itu-telecom-freq** and **g8275dot2-2016** profiles do not apply when the *clock-id* is **csm**)

master-only

Syntax

master-only {**true** | **false**}

Context

config>system>ptp>clock>port

config>system>ptp>clock>ptp-port

Description

This command prevents the local port from ever entering the timeReceiver state. This ensures that the 7705 SAR never draws synchronization from an attached external device.

This command only applies when the profile command is set to **g8275dot1-2014** or **g8275dot2-2016**.

If the **clock-type** command is set to **ordinary slave**, the **master-only** value is set to **false** and cannot be changed. Similarly, if the **clock-type** command is set to **ordinary master**, the **master-only** value is set to **true** and cannot be changed.

Default

true (when the PTP **clock-type** is set to **boundary**)

profile

Syntax

profile {**primary** | *name*}

Context

config>system>ptp>clock>port

Description

This command assigns the profile to be used for communications with the port or peer.

If **primary** profile is specified, the PTP port uses the profile configured by the **profile** command in the **config>system>ptp>clock** context. If an alternate profile name is specified, the PTP port uses the alternate profile configured by the **profile** command in the **config>system>ptp>clock>alternate-profile** context. The alternate profile must already be created.

Default

primary

Parameters

primary

the system uses the primary profile configured in the **config>system>ptp>clock** context

name

specifies the name of an existing alternate profile to use

time-inaccuracy-override

Syntax

time-inaccuracy-override *time-inaccuracy-override*

no time-inaccuracy-override

Context

config>system>ptp>clock>port

Description

This command overrides the system-generated value for the PTP clock's time inaccuracy with a specified value. The clock's time inaccuracy value is added to the total time inaccuracy value in IEEE_C37_238 TLVs sent to downstream clocks in Announce messages. If there is no time inaccuracy override configured, the system uses 50 ns as the default for boundary clocks.

This command is applicable only for boundary clocks and only when the profile is configured as **c37dot238-2017**.

The **no** form of this command removes the time inaccuracy override value.

Default

no time-inaccuracy-override

Parameters

time-inaccuracy-override

specifies the time inaccuracy of the PTP clock in nanoseconds, to be added to the total time inaccuracy in the IEEE_C37_238 TLV

> **Values**   0 to 10000000

priority1

Syntax

priority1 *priority-value*

no priority1

Context

config>system>ptp>clock

Description

This command configures the first priority value of the local clock. This value is used by the BTCA to determine which clock should provide timing for the network. It is also used as the advertised value in Announce messages and as the local clock value in data set comparisons.

When the profile command is set to **g8275dot1-2014** or **g8275dot2-2016**, the priority1 value is set to the default value of 128 and cannot be changed.

The **no** form of the command returns the configuration to the default value.

Default

128

Parameters

priority

specifies the priority1 value of the local clock

> **Values**   0 to 255

priority2

Syntax

priority2 *priority-value*

no priority2

Context

config>system>ptp>clock

Description

This command configures the second priority value of the local clock. This value is used by the BTCA to determine which clock should provide timing for the network. It is also used as the advertised value in Announce messages and as the local clock value in data set comparisons.

When the profile command is set to **g8275dot1-2014** or **g8275dot2-2016** and the clock-type is configured as **ordinary slave**, the **priority2** value is set to the default value of 255 and cannot be changed.

The **no** form of the command returns the configuration to the default value.

Default

128, when the clock type is configured as **ordinary master** or **boundary**

255, when the clock type is configured as **ordinary slave**

Parameters

priority

> specifies the priority2 value of the local clock

> > **Values**   0 to 255 when the profile is configured as **ieee1588-2008**, **iec-61850-9-3-2016**, or **c37dot238-2017**, or when the profile is configured as **g8275dot1-2014** or **g8275dot2-2016** and the clock type is configured as **ordinary master** or **boundary**

profile

Syntax

profile {**c37dot238-2017**| **iec-61850-9-3-2016** | **ieee1588-2008** | **itu-telecom-freq** | **g8275dot1-2014** | **g8275dot2-2016**}

no profile

Context

config>system>ptp>clock

Description

This command defines the specification rules to be used by PTP. Configuring the profile changes the BTCA and SSM/QL mappings to match the settings in the specification. The profile can only be changed when PTP is shut down. Changing the profile changes the domain to the default value of the new profile.

The **no** form of the command returns the configuration to the default setting.

Default

ieee1588-2008

Parameters

g8275dot1-2014

> configures the PTP profile to follow the ITU G.8275.1 specification rules

g8275dot2-2016

> configures the PTP profile to follow the ITU G.8275.2 specification rules; this option is only available when the *clock-id* parameter value is 1 to 16

ieee1588-2008

> configures the PTP profile to follow the IEEE 1588-2008 specification rules

itu-telecom-freq

> configures the PTP profile to follow the ITU G.8265.1 specification rules; this option is only available when the *clock-id* parameter value is 1 to 16

iec-61850-9-3-2016

> configures the PTP profile to follow the IEC/IEEE 61850-9-3 specification rules; this option is only available when the *clock-id* parameter value is **csm**

c37dot238-2017

> configures the PTP profile to follow the C37.238-2017 specification rules; this option is only available when the *clock-id* parameter value is **csm**

ptp-port

Syntax

ptp-port *port-id*

Context

config>system>ptp>clock

Description

This command configures an IEEE 1588v2 logical port in the system. It also enables the context to configure parameters for IEEE 1588v2. PTP ports are created when the clock type is set with the clock-type command.

This command is only available when the *clock-id* parameter value is 1 to 16.

When the clock type is set to **ordinary slave**, one port with 2 peers is created. When the clock type is set to **ordinary master**, one port with 50 peers is created. When the clock type is set to boundary clock, 50 ports each with 1 peer are created.

> **Note:** When the clock type is set to transparent, PTP is associated with all ports on the 7705 SAR-M, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, or 7705 SAR-X, rather than on individual ports, because transparent clock is a system-wide setting.

Default

n/a

Parameters

port-id

> specifies the PTP port ID

Values   1 to 50

peer

Syntax
peer *peer-id*

Context
config>system>ptp>clock>ptp-port

Description
This command enables the context to configure parameters associated with remote PTP peers such as grandmaster clocks.

For ordinary timeReceiver clocks, 2 peers are automatically created. For ordinary timeTransmitter clocks, 50 peers are automatically created. For boundary clocks, 1 peer per PTP port is automatically created.

The **no** form of the command removes the IP address from the PTP peer.

Default
n/a

Parameters
peer-id

specifies the PTP peer ID

Values   1 to 2 (ordinary timeReceiver)
1 to 50 (ordinary timeTransmitter)
1 (boundary)

ip-address

Syntax
ip-address {*ip-address* | *ipv6-address*}

no ip-address

Context
config>system>ptp>clock>ptp-port>peer

Description
This command configures a remote PTP peer address and enables the context to configure parameters for the remote PTP peer.

Up to two remote PTP peers may be configured on a PTP port.

The **no** form of the command removes the IP address from the PTP peer.

Default

n/a

Parameters

ip-address

specifies the IPv4 or IPv6 address of the remote peer

unicast-negotiate

Syntax

[**no**] **unicast-negotiate**

Context

config>system>ptp>clock>ptp-port

Description

This command specifies whether the timeReceiver clock is to initiate a unicast request to the timeTransmitter clock or wait for Announce and Synchronization messages from the timeTransmitter clock.

The **no** form of this command disables **unicast-negotiate**. In this case, the user must specify the timeReceiver clock information when configuring the 7705 SAR timeTransmitter node in order for communication between the timeReceiver clock and timeTransmitter clock to take place.

Default

unicast-negotiate

source-interface

Syntax

source-interface *ip-int-name*

no source-interface

Context

config>system>ptp>clock

Description

This command defines the IP interface that provides the IEEE 1588 packets to the clock recovery mechanism on the adapter card or port. The interface must be PTP-enabled.

This command only applies when the *clock-id* parameter value is 1 to 16.

If the *ip-int-name* refers to a loopback or system address, the remote peer can send packets toward any network IP interface. If the *ip-int-name* refers to an interface that is associated with a physical port or VLAN, the remote peer must send packets to ingress on that particular IP interface.

Default

n/a

Parameters

ip-int-name

specifies the IP interface used by the PTP timeReceiver clock

tx-while-sync-uncertain

Syntax

[no] **tx-while-sync-uncertain**

Context

config>system>ptp>clock

Description

This command enables or disables the transmission of Announce messages to downstream clocks if the PTP network has not yet stabilized. In some cases, it may be important for a downstream boundary clock or timeReceiver clock to know whether the PTP network has stabilized or is still "synchronization uncertain".

To indicate the synchronization certainty state, the synchronizationUncertain flag in the Announce message is set to TRUE if the clock is in a "synchronization uncertain" state and is set to FALSE if the clock is in a "synchronization certain" state.

However, because the synchronizationUncertain flag is newly agreed upon in standards, most base station timeReceiver clocks do not look at this bit. Therefore, to ensure that the downstream clocks are aware of the state of the network, the PTP clock may be configured to transmit Announce and Sync messages only if the clock is in a "synchronization certain" state. This is done using the **no** form of this command.

Default

tx-while-sync-uncertain

use-node-time

Syntax

[no] **use-node-time**

Context

config>system>ptp>clock

Description

This command determines whether the PTP clock will generate event messages based on system time.

The **use-node-time** command allows a router with a PTP timeTransmitter or boundary clock to distribute ToD/phase from the system time referenced from GNSS or another configured PTP clock. A router with a single PTP clock configured as a boundary clock with multiple peers does not require **use-node-time** to enable ToD/phase distribution capability. For a 7705 SAR with an active GNSS receiver port, PTP boundary clocks in **use-node-time** mode will function similar to a grandmaster clock with GNSS traceability.

This command only applies to timeTransmitter or boundary clocks when:

- the profile setting for the PTP clock is **ieee1588-2008** (default configuration), **g8275dot1-2014**, or **g8275dot2-2016** (see the profile command for the **config>system>ptp>**clock context)
- the *clock-id* parameter value is 1 to 16

Default

no use-node-time

use-node-time when the profile for the timeTransmitter clock is configured as **g8275dot1-2014**

6.13.2.2 Administration commands

- System administration commands
- High availability (redundancy) commands

6.13.2.2.1 System administration commands

admin

Syntax

admin

Context

<ROOT>

Description

This command enables the context to configure administrative system commands. Only authorized users can execute the commands in the **admin** context.

Default

n/a

debug-save

Syntax

   debug-save *file-url*

Context

   admin

Description

   This command saves existing debug configuration. Debug configurations are not preserved in configuration saves.

Default

   n/a

Parameters

   file-url

   the file URL location to save the debug configuration (see Table 14: URL types and syntax for parameter descriptions)

disconnect

Syntax

   disconnect [**address** *ip-address* | **username** *user-name* | **session-id** *session-id* | {**console** | **telnet** | **ftp** | **ssh** | **mct**}]

Context

   admin

Description

   This command disconnects a user from a console, Telnet, FTP, SSH, SFTP, or MPT craft terminal (MCT) session.

   If any of the console, Telnet, FTP, SSH, or MCT options are specified, only the respective sessions are affected. The **ssh** keyword disconnects all users connected to the node via SSH or SFTP, including all sessions of each SSH connection belonging to those users.

   If no console, Telnet, FTP, SSH, or MCT options are specified, all sessions from the IP address or from the specified user are disconnected.

   If an SSH session is specified, only that SSH session under an SSH connection is disconnected. Each SSH connection supports up to 5 sessions. Each session has a corresponding channel ID. If multiple sessions are under one connection, the initial session corresponds to channel ID 0. This session cannot be fully disconnected until all other sessions belonging to that SSH connection are also disconnected.

When a user is disconnected from a session, any task that the user is executing is terminated. FTP files accessed by the user are not removed. A major severity security log event is created, specifying what was terminated and by whom.

Default

n/a — no disconnect options are configured

Parameters

ip-address

the IP address to disconnect

session-id

the ID of the session to disconnect

user-name

the name of the user

console

disconnects the console session

telnet

disconnects the Telnet session

ftp

disconnects the FTP session

ssh

disconnects the SSH or SFTP session

mct

disconnects the MCT session

display-config

Syntax

display-config [**detail** | **index**]

Context

admin

Description

This command displays the system's running configuration.

By default, only non-default settings are displayed.

Specifying the **detail** option displays all default and non-default configuration parameters.

Parameters

detail

displays default and non-default configuration parameters

index

> displays only persistent indexes

reboot

Syntax

reboot [**active** | **standby**] | [**upgrade**] [**now**]

Context

admin

Description

This command reboots the router including redundant CSMs or upgrades the boot ROMs.

If no options are specified, the user is prompted to confirm the reboot operation. For example:

```
ALU-1>admin# reboot
Are you sure you want to reboot (y/n)?
```

If the **now** option is specified, no boot confirmation messages appear.

Parameters

active

> keyword to reboot the active CSM

>> **Default**   active

standby

> keyword to reboot the standby CSM

>> **Default**   active

upgrade

> enables card firmware to be upgraded during chassis reboot. The 7705 SAR and the boot.ldr support functionality to perform automatic firmware upgrades on CSMs. The automatic upgrade must be enabled in the 7705 SAR Command Line Interface (CLI) when rebooting the system.

> When the **upgrade** keyword is specified, a chassis flag is set for the Boot Loader (boot.ldr) and on the subsequent boot of the 7705 SAR on the chassis, any firmware images on CSMs requiring upgrading will be upgraded automatically.

> If a 7705 SAR is rebooted with the "admin reboot" command (without the "upgrade" keyword), the firmware images are left intact.

> Any CSMs that are installed in the chassis will be upgraded automatically. For example, if a card is inserted with down revision firmware as a result of a card hot swap with the latest OS version running, the firmware on the card will be automatically upgraded before the card is brought online.

If the card firmware is upgraded automatically, a CHASSIS "cardUpgraded" (event 2032) log event is generated. The corresponding SNMP trap for this log event is "tmnxEqCardFirmwareUpgraded".

During any firmware upgrade, automatic or manual, it is imperative that during the upgrade procedure:

- power must NOT be switched off or interrupted

- the system must NOT be reset

- no cards are inserted or removed

Any of the above conditions may render cards inoperable requiring a return of the card for resolution.

The time required to upgrade the firmware on the cards in the chassis depends on the number of cards to be upgraded. On system reboot, the firmware upgrades can take from approximately 3 minutes (for a minimally loaded 7705 SAR) to 8 minutes (for a fully loaded 7705 SAR chassis), after which the configuration file will be loaded. The progress of the firmware upgrades can be monitored at the console. Inserting a single card requiring a firmware upgrade in a running system generally takes less than 2 minutes before the card becomes operationally up.

now

forces a reboot of the router immediately without an interactive confirmation

save

Syntax

save [*file-url*] [**detail**] [**index**]

Context

admin

Description

This command saves the running configuration to a configuration file. For example:

```
ALU-1>admin# save ftp://test:test@192.168.x.xx/./100.cfg
Saving configuration .........Completed.
```

By default, the running configuration is saved to the primary configuration file.

Parameters

file-url

the file URL location to save the configuration file (see Table 14: URL types and syntax for parameter descriptions)

> **Default**   the primary configuration file location

detail

saves both default and non-default configuration parameters

Default   saves non-default configuration parameters

index

forces a save of the persistent index file regardless of the persistent status in the BOF file. The index option can also be used to avoid an additional boot required while changing your system to use the persistence indexes.

enable-tech

Syntax

[**no**] **enable-tech**

Context

admin

Description

This command enables the shell and kernel commands.

> **Note:** This command should only be used with authorized direction from the Nokia Technical Assistance Center (TAC).

tech-support

Syntax

tech-support *file-url*

Context

admin

Description

This command creates a system core dump.

If the *file-url* is omitted, and a ts-location has previously been defined, the tech-support file will get an automatic 7705 SAR generated filename based on the system name, date, and time, and the file will be saved to the directory indicated by the configured **ts-location**.

The format of the auto-generated filename is ts-xxxxx.yyyymmdd.hhmmUTC.dat, where:

* xxxxx is the system name with any special characters expanded to avoid problems with file systems (for example, a period (".") is expanded to "%2E.")

* yyyymmdd is the date, with leading zeros on year, month, and day

* hhmm are the hours and minutes in UTC time (24-hour format, always 4 characters, with leading zeros on the hours and minutes)

Note: This command should only be used with authorized direction from the Nokia Technical Assistance Center (TAC).

Parameters

file-url

the file URL location to save the binary file (see Table 14: URL types and syntax for parameter descriptions)

ts-location

Syntax

ts-location *file-url*

no ts-location

Context

config>system>security>tech-support

Description

This command specifies a location for the auto-generated filename that is created if the *file-url* parameter is not used in the tech-support command. The file is automatically assigned a name and saved to the configured location only if this **ts-location** command has first been configured; otherwise, the *file-url* parameter must be configured in the **tech-support** command to provide this information. The directory specified for the **ts-location** is not automatically created by the 7705 SAR; it must already exist.

Parameters

file-url

the file URL location to save the binary file (see Table 14: URL types and syntax for parameter descriptions)

update

Syntax

update boot-loader *file-url*

Context

admin

Description

This command upgrades the boot loader file on the system. The command checks that the new boot.ldr is a valid image and that it is at least a minimum supported variant for the hardware platform on which it is being loaded. When this has been verified, the command overwrites the boot.ldr file that is stored on the system.

Nokia recommends that the boot loader file on all 7705 SAR platforms be upgraded using this command. This command is mandatory on all 7705 SAR platforms that do not have a removable compact flash drive and is part of a mechanism that protects the boot loader file from accidental overwrites on these platforms.

> ⚠️ **WARNING:** The file upgrade command takes several minutes to complete. Do not reset or power down the system, or insert or remove cards or modules, while the upgrade is in progress, as this could render the system inoperable.

See the latest 7705 SAR Software Release Notes, "Standard Software Upgrade Procedure" section, for complete instructions.

Parameters

file-url

the file URL location to use for upgrading the boot.ldr file (see Table 14: URL types and syntax for parameter descriptions)

> **Default**   the new boot.ldr file location

6.13.2.2.2 High availability (redundancy) commands

redundancy

Syntax
redundancy

Context
admin

config

Description
This command enters the context to allow the user to perform redundancy operations.

force-switchover

Syntax
force-switchover [**now**]

Context
admin>redundancy

Description
This command forces a switchover to the standby CSM card. The primary CSM reloads its software image and becomes the secondary CSM.

Parameters

now

forces the switchover to the redundant CSM card immediately

switchover-exec

Syntax

switchover-exec *file-url*

no switchover-exec

Context

config>system

Description

This command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CSM card. A switchover can happen because of a fatal failure or by manual action.

The CLI script file can contain commands for environment settings, debug settings, and other commands not maintained by the configuration redundancy.

When the *file-url* parameter is not specified, no CLI script file is executed.

Default

n/a

Parameters

file-url

specifies the location and name of the CLI script file (see Table 14: URL types and syntax for parameter descriptions)

synchronize

Syntax

synchronize {**boot-env** | **config**}

Context

admin>redundancy

config>redundancy

Description

This command performs a synchronization of the standby CSM's images and/or config files to the active CSM. Either the **boot-env** or **config** parameter must be specified.

In the **admin>redundancy** context, this command performs a manually triggered standby CSM synchronization.

In the **config>redundancy** context, this command performs an automatically triggered standby CSM synchronization.

When the standby CSM takes over operation following a failure or reset of the active CSM, it is important to ensure that the active and standby CSMs have identical operational parameters. This includes the saved configuration and CSM images.

The active CSM ensures that the active configuration is maintained on the standby CSM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CSM.

If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

Default

n/a for admin — redundancy context

enabled for config — redundancy context

Parameters

boot-env

synchronizes all files required for the boot process (loader, BOF, images, and configuration files

config

synchronizes only the primary, secondary, and tertiary configuration files

Default   config

cert-sync

Syntax

[no] **cert-sync**

Context

config>redundancy

Description

This command automatically synchronizes the certificate/CRL/key when importing the certificate or generating the key. If a new compact flash card is inserted into the backup CSM, the system will synchronize the whole **cf3:/system-pki** directory from the active CSM.

Default

cert-sync

multi-chassis

Syntax

multi-chassis

Context

config>redundancy

Description

This command enables the context to configure multi-chassis parameters.

peer

Syntax

[**no**] **peer** *ip-address* [**create**]

Context

config>redundancy>multi-chassis

Description

This command configures a multi-chassis redundancy peer.

Parameters

ip-address

specifies a peer IP address. A multicast address is not allowed.

create

keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the **create** keyword.

authentication-key

Syntax

authentication-key [*authentication-key* | *hash-key*] [**hash** | **hash2**]

no authentication-key

Context

config>redundancy>multi-chassis>peer

Description

This command configures the authentication key used between this node and the multi-chassis peer. The authentication key can be any combination of letters or numbers.

Parameters

authentication-key

specifies the authentication key. Allowed values are any string up to 20 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

hash-key

specifies the hash key. The key can be any combination of ASCII characters up to 33 (hash1-key) or 55 (hash2-key) characters in length (encrypted). If spaces are used in the string, the entire string must be enclosed within double quotes.

hash

specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2

specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone. This means that a hash2 encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

description

Syntax

description *description-string*

no description

Context

config>redundancy>multi-chassis>peer

Description

This command configures a text description and associates it with a configuration context to help identify the content in a configuration file.

The **no** form of the command removes the string from the configuration.

Default

n/a

Parameters

description-string

specifies the text description

> **Values**   any string of 7-bit ASCII characters, up to 80 characters in length; the entire string must be enclosed in double quotes if it contains any special characters

mc-firewall

Syntax

[**no**] **mc-firewall**

Context

config>redundancy>multi-chassis>peer

Description

This command enables the context to configure parameters on the multi-chassis link (MCL), which enables the multi-chassis firewall function.

The **no** form of this command administratively disables multi-chassis firewall. The **no mc-firewall** command can only be issued when multi-chassis firewall is shut down.

Default

n/a

boot-timer

Syntax

boot-timer *interval*

no boot-timer

Context

config>redundancy>multi-chassis>peer>mc-firewall

Description

This command configures a boot timer interval for the MCL. This command applies when either router reboots. It specifies how long the multi-chassis firewall protocol attempts to establish a connection between the peers before assuming a failure of the remote peer. This is different from the keepalive mechanism that is used once the peer-to-peer communication has been established. If the boot timer interval expires before a connection between the two peers is established, both multi-chassis firewall peers will return to standalone firewall operation.

The **no** form of this command resets the interval to the default value.

Default

300 s

Parameters

interval

the boot timer interval, in seconds

Values   1 to 600

encryption

Syntax

[**no**] **encryption**

Context

config>redundancy>multi-chassis>peer>mc-firewall

Description

This command enables the context to configure encryption and/or authentication algorithms to secure the multi-chassis firewall link. The **no** form of the command disables encryption.

Default

no encryption

active-outbound-sa

Syntax

active-outbound-sa *active-outbound-sa*

no active-outbound-sa

Context

config>redundancy>multi-chassis>peer>mc-firewall>encryption

Description

This command identifies the active security association (SA) to be used for encrypting packets on the multi-chassis firewall link. On egress, only the active outbound SA is used to encrypt packets. On ingress, both SAs can be used to decrypt the arriving packets; this mechanism is used for rolling over the encryption and authentication keys.

The **no** form of the command resets the parameter to its default value.

Default

no active-outbound-sa

Parameters

active-outbound-sa

the index number (SPI) of the active security association

Values 1 to 1023

authen-algorithm

Syntax

authen-algorithm *authen-algorithm*

no authen-algorithm

Context

config>redundancy>multi-chassis>peer>mc-firewall>encryption

Description

This command configures the authentication algorithm for the MCL.

The **no** form of the command resets the parameter to its default value.

Default

sha256

Parameters

authen-algorithm

the algorithm used to authenticate the MCL

Values sha256 or sha512

encryp-algorithm

Syntax

encryp-algorithm *encryp-algorithm*

no encryp-algorithm

Context

config>redundancy>multi-chassis>peer>mc-firewall>encryption

Description

This command configures the encryption algorithm for the MCL.

The **no** form of the command resets the parameter to its default value.

Default

aes128

Parameters

encryp-algorithm

the algorithm used to encrypt the MCL

Values   aes128 or aes256

security-association

Syntax

security-association spi *spi* **authentication-key** *authentication-key* **encryption-key** *encryption-key* [**hash** | **hash2**]

no security-association spi *spi*

Context

config>redundancy>multi-chassis>peer>mc-firewall>encryption

Description

This command creates a security association index for encryption of the MCL. The command is also used to enter the authentication and encryption key values for the security association, or to delete the security association. A security association contains the keys needed to encrypt and authenticate the link and is identified using an SPI. There can be two security association indexes under encryption. These two indexes can be used for rolling over the keys.

The **no** form of the command deletes the SPI.

Default

no security-association spi

Parameters

spi

the index for this security association

Values   1 to 1023

authentication-key

the authentication key for the security association, either in hexadecimal format (up to 128 hexadecimal nibbles) or as a hash key.

Values   0x0 to 0xFFFFFFFF or *hash-key*

encryption-key

the encryption key for the security association, either in hexadecimal format (up to 64 hexadecimal nibbles) or as a hash key

Values   0x0 to 0xFFFFFFFF or *hash-key*

hash-key

> the hash key. The key can be any combination of ASCII characters up to 33 (hash1-key) or 55 (hash2-key) characters in length (encrypted). If spaces are used in the string, the entire string must be enclosed within double quotes.

hash

> specifies that the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2

> specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone. This means that a hash2 encrypted variable cannot be copied and pasted. If the **hash2** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hold-on-neighbor-failure

Syntax

hold-on-neighbor-failure *multiplier*

no hold-on-neighbor-failure

Context

config>redundancy>multi-chassis>peer>mc-firewall

Description

This command specifies the number of keepalive intervals that the local router will wait for packets from the multi-chassis firewall peer before assuming that the remote router has failed. If the configured number of intervals is reached before the local router receives packets from the peer, both routers will return to standalone firewall operation.

The **no** form of this command resets the number of intervals to the default value.

Default

3

Parameters

multiplier

> the number of keepalive intervals

Values   2 to 25

keep-alive-interval

Syntax

keep-alive-interval *interval*

no keep-alive-interval

Context

config>redundancy>multi-chassis>peer>mc-firewall

Description

This command sets the interval at which keepalive messages are exchanged between the two routers participating in a multi-chassis firewall. These keepalive messages are used to determine whether the remote router has failed.

The **no** form of the command resets the interval to its default value.

Default

10 (1 s)

Parameters

interval

the time interval expressed in deciseconds

Values 5 to 500

system-priority

Syntax

system-priority *value*

no system-priority

Context

config>redundancy>multi-chassis>peer>mc-firewall

Description

This command configures the system priority for the routers participating in a multi-chassis firewall. The router configured with the lowest value becomes the master. If system priority is the same for both routers, the router with the lowest system ID (chassis MAC address) becomes the master.

The **no** form of this command resets the system priority to the default value.

Default

0

Parameters

value

the priority of the local multi-chassis firewall peer

Values   1 to 255

mc-lag

Syntax

[**no**] **mc-lag**

Context

config>redundancy>multi-chassis>peer

Description

This command enables the context to configure multi-chassis LAG parameters.

The **no** form of this command administratively disables multi-chassis LAG. The **no mc-lag** command can only be issued only when MC-LAG is shut down.

Default

n/a

hold-on-neighbor-failure

Syntax

hold-on-neighbor-failure *multiplier*

no hold-on-neighbor-failure

Context

config>redundancy>multi-chassis>peer>mc-lag

Description

This command sets the number of keep alive intervals the standby 7705 SAR will wait for packets from the active node before assuming a redundant neighbor node failure. This delay in switchover operation is required to accommodate different factors influencing node failure detection rate, such as IGP convergence or high availability switchover times, and to prevent the standby node from take over prematurely.

The **no** form of the command sets this parameter to its default value.

Default

3

Parameters

multiplier

> a multiplier of the keepalive interval is used to set the number of keepalive intervals that the standby node will wait for packets from the active node before assuming a redundant-neighbor node failure.

> **Values**   2 to 25

keep-alive-interval

Syntax

keep-alive-interval *interval*

no keep-alive-interval

Context

config>redundancy>multi-chassis>peer>mc-lag

Description

This command sets the interval at which keepalive messages are exchanged between two systems participating in an MC-LAG. These keepalive messages are used to determine remote-node failure.

The **no** form of the command sets the interval to its default value.

Default

10 (1s)

Parameters

interval

> the time interval expressed in deciseconds

> **Values**   5 to 500

lag

Syntax

lag *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *lag-id*] **system-priority** *system-priority*

no lag *lag-id*

Context

config>redundancy>multi-chassis>peer>mc-lag

Description

This command defines a LAG that is forming a redundant pair for MC-LAG with a LAG configured on the given peer. The same LAG group can be defined only in the scope of one peer.

The same **lacp-key**, **system-id**, and **system-priority** must be configured on both nodes of the redundant pair in order for MC-LAG to become operational. If there is a mismatch, MC-LAG remains operationally down.

Default

n/a

Parameters

lag-id

> the LAG identifier, expressed as a decimal integer. You must specify the LAG ID. Specifying the *lag-id* allows a mismatch between *lag-id* on the redundant pair. If you have two existing nodes that already have LAG IDs that do not match, and an MC-LAG is to be created using these nodes, you must specify the correct **remote-lag** *lag-id* so that the matching MC-LAG group can be found. If no matching MC-LAG group can be found between neighbor systems, the individual LAGs will operate as usual (no MC-LAG operation is established).

> > **Values**   1 to 32

admin-key

> specifies a 16-bit key that needs to be configured in the same manner on both sides of the MC-LAG in order for the MC-LAG to be operationally up

> > **Values**   1 to 65535

system-id

> specifies a 6-bit value expressed in the same notation as a MAC address

> > **Values**   xx:xx:xx:xx:xx:xx -xx[00 to FF]

remote-lag *lag-id*

> specifies the LAG ID on the remote system

> > **Values**   1 to 200

system-priority

> specifies the system priority to be used in the context of the MC-LAG. The partner system will consider all ports using the same **lacp-key**, **system-id**, and **system-priority** as part of the same LAG.

> > **Values**   1 to 65535

source-address

Syntax

source-address *ip-address*

no source-address

Context

config>redundancy>multi-chassis>peer

Description

This command specifies the source address used to communicate with the multi-chassis peer.

Parameters

ip-address

specifies the source address used to communicate with the multi-chassis peer

Values   a.b.c.d (no multicast address)

6.13.2.3 Show commands

📝   **Note:**

- The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.
- The IEEE 1588 Working Group has introduced the terms timeTransmitter and timeReceiver as alternatives to the former master/slave terminology used in PTP. This section uses the terms **master** and **slave** only when referring to the PTP CLI commands or command outputs.

connections

Syntax

connections [**address** *ip-address*] [**port** *port-number*] [**detail**]

Context

show>system

Description

This command displays UDP and TCP connection information.

If no command line options are specified, a summary of the TCP and UDP connections displays.

Parameters

ip-address

displays only the connection information for the specified IP address or interface name

port-number

  displays only the connection information for the specified port number

   Values 0 to 65535

detail

  appends TCP statistics to the display output

Output

The following output is an example of UDP and TCP connection information, and Table 36: System connections field descriptions describes the fields.

Output example

```
A:ALU-1# show system connections
===============================================================================
Connections :
===============================================================================
Proto    RecvQ    TxmtQ Local Address                         State
                    MSS Remote Address                        vRtrID
-------------------------------------------------------------------------------
TCP          0        0 10.0.0.0.21                           LISTEN
                   1024 10.0.0.0.0                            0
TCP          0        0 10.0.0.0.23                           LISTEN
                        10.0.0.0.0                            0
TCP          0        0 10.0.0.0.179                          LISTEN
                        10.0.0.0.0                            0
TCP          0        0 10.0.0.xxx.51138                      SYN_SENT
                        10.0.0.104.179                        4095
TCP          0        0 10.0.0.xxx.51139                      SYN_SENT
                        10.0.0.91.179                         4095
TCP          0        0 10.10.10.xxx.646                      LISTEN
                        10.0.0.0.0                            0
TCP          0        0 10.10.10.xxx.646                      ESTABLISH
                        10.10.10.104.49406                    4095
TCP          0        0 11.1.0.1.51140                        SYN_SENT
                        11.1.0.2.179                          4095
TCP          0      993 192.168.x.xxx.23                      ESTABLISHED
                        192.168.x.xx.xxxx                     4095
UDP          0        0 10.0.0.0.123                          ---
                        10.0.0.0.0                            0
UDP          0        0 10.0.0.0.646                          ---
                        10.0.0.0.0                            0
UDP          0        0 10.0.0.0.17185                        ---
                        0.0.0.0.0                             0
UDP          0        0 10.10.10.xxx.646                      ---
                        10.0.0.0.0                            0
UDP          0        0 192.0.0.1.50130                       ---
                        192.0.0.1.17185                       4095
-------------------------------------------------------------------------------
No. of Connections: 14
===============================================================================
A:ALU-1#
```

Output example (detailed)

```
A:ALU-1# show system connections detail
-------------------------------------------------------------------------------
 TCP Statistics
-------------------------------------------------------------------------------
```

```
packets sent                              : 659635
data packets                              : 338982 (7435146 bytes)
data packet retransmitted                 : 73 (1368 bytes)
ack-only packets                          : 320548 (140960 delayed)
URG only packet                           : 0
window probe packet                       : 0
window update packet                      : 0
control packets                           : 32
packets received                          : 658893
acks                                      : 338738 for (7435123 bytes)
duplicate acks                            : 23
ack for unsent data                       : 0
packets received in-sequence              : 334705 (5568368 bytes)
completely duplicate packet               : 2 (36 bytes)
packet with some dup. data                : 0 (0 bytes)
out-of-order packets                      : 20 (0 bytes)
packet of data after window               : 0 (0 bytes)
window probe                              : 0
window update packet                      : 3
packets received after close              : 0
discarded for bad checksum                : 0
discarded for bad header offset field     : 0
discarded because packet too short        : 0
connection request                        : 4
connection accept                         : 24
connections established (including accepts) : 27
connections closed                        : 26 (including 2 drops)
embryonic connections dropped             : 0
segments updated rtt                      : 338742 (of 338747 attempts)
retransmit timeouts                       : 75
connections dropped by rexmit timeout     : 0
persist timeouts                          : 0
keepalive timeouts                        : 26
keepalive probes sent                     : 0
connections dropped by keepalive          : 1
pcb cache lookups failed                  : 0
connections dropped by bad md5 digest     : 0
connections dropped by enhanced auth      : 0
path mtu discovery backoff                : 0
===============================================================================
A:ALU-1#
```

Table 36: System connections field descriptions

Label	Description
Proto	The socket protocol, either TCP or UDP
RecvQ	The number of input packets received by the protocol
TxmtQ	The number of output packets sent by the application
Local Address	The local address of the socket. The socket port is separated by a period.
Remote Address	The remote address of the socket. The socket port is separated by a period.
State	Listen — the protocol state is in the listen mode

Label	Description
	Established — the protocol state is established
MSS	The TCP maximum segment size
vRtrID	The virtual router identifier:
	vRtrID 0 — listens for connections in all routing instances, including the base and management VRFs
	vRtrID 1 — base routing instance
	vRtrID 4095 — management routing instance

cpu

Syntax

cpu [**sample-period** *seconds*]

Context

show>system

Description

This command displays CPU usage per task over a sample period.

Parameters

seconds

the number of seconds over which to sample CPU task usage

Default 1

Values 1 to 10

Output

The following output is an example of system CPU information, and Table 37: System CPU field descriptions describes the fields.

Output example

```
A:ALU-1# show system cpu sample-period 2
===============================================================================
CPU Utilization (Sample period: 2 seconds)
===============================================================================
Name                              CPU Time      CPU Usage      Capacity
                                  (uSec)                       Usage
-------------------------------------------------------------------------------
BFD                                 10,098          0.07%         0.37%
BGP                                    341         ~0.00%         0.01%
Cards & Ports                       55,154          0.39%         0.81%
DHCP Server                            352         ~0.00%         0.01%
```

```
ICC                                         7,818          0.05%          0.20%
IGMP/MLD                                    3,511          0.02%          0.17%
IOM                                       170,517          1.22%          3.47%
IP Stack                                   14,371          0.10%          0.23%
IS-IS                                      19,893          0.14%          0.99%
ISA                                         5,822          0.04%          0.29%
LDP                                         1,746          0.01%          0.08%
Logging                                        94         ~0.00%         ~0.00%
MPLS/RSVP                                  16,146          0.11%          0.60%
Management                                 12,337          0.08%          0.40%
Microwave                                      43         ~0.00%         ~0.00%
OAM                                         1,100         ~0.00%          0.05%
OSPF                                          610         ~0.00%          0.02%
PIM                                           418         ~0.00%          0.02%
RIP                                             0          0.00%          0.00%
RTM/Policies                                    0          0.00%          0.00%
Redundancy                                 27,293          0.19%          1.05%
Security                                    1,858          0.01%          0.06%
Services                                    4,978          0.03%          0.08%
Snmp Daemon                                     0          0.00%          0.00%
Stats                                           0          0.00%          0.00%
System                                    247,815          1.77%          3.71%
VRRP                                        2,443          0.01%          0.07%

-----------------------------------------------------------------------------
Total                                  13,950,560        100.00%
   Idle                                13,335,735         95.59%
   Usage                                  614,825          4.40%
Busiest Core Utilization                  164,574          8.25%
=============================================================================
A:ALU-1#
```

Table 37: System CPU field descriptions

Label	Description
CPU Utilization	The total amount of CPU time
Name	The process or protocol name
CPU Time (uSec)	The CPU time that each process or protocol has used in the specified sample time
CPU Usage	The sum of CPU usage of all the processes and protocols
Capacity Usage	Displays the level at which the specified service is being used. When this number reaches 100%, this part of the system is busied out. There may be extra CPU cycles still left for other processes, but this service is running at capacity. This column does not reflect the true CPU utilization value; that data is available in the CPU Usage column. This column shows the busiest task in each group, where "busiest" is defined as either actually running or blocked attempting to acquire a lock.

cron

Syntax

cron

Context

show>system

Description

This command enters the show CRON context.

schedule

Syntax

schedule [*schedule-name*] [**owner** *owner-name*]

Context

show>system>cron

Description

This command displays CRON schedule parameters.

Parameters

schedule-name

      displays information for the specified schedule name

owner-name

      displays information for the specified schedule owner associated with the schedule name

Output

The following output is an example of CRON schedule information, and Table 38: CRON schedule field descriptions describes the fields.

Output example

```
A:ALU-1# show system cron schedule test
===============================================================================
CRON Schedule Information
===============================================================================
Schedule                      : test
Schedule owner                : TiMOS CLI
Description                    : none
Administrative status         : enabled
Operational status            : enabled
Script Policy                 : test_policy
Script Policy Owner           : TiMOS CLI
Script                        : test_script
Script Owner                  : TiMOS CLI
Script source location        : ftp://*****:******@192.168.15.1/home/testlab_bgp
```

```
                               /cron/test1.cfg
  Script results location    : ftp://*****:******@192.168.15.1/home/testlab_bgp
                               /cron/res
  Schedule type              : periodic
  Interval                   : 0d 00:01:00 (60 seconds)
  Repeat count               : infinite
  Next scheduled run         : 0d 00:00:42
  End time                   : 2018/12/17 12:00:00
  Weekday                    : friday
  Month                      : none
  Day of month               : none
  Hour                       : none
  Minute                     : none
  Number of schedule runs    : 10
  Last schedule run          : 2018/12/17 11:20:00
  Number of schedule failures  : 0
  Last schedule failure      : no error
  Last failure time          : never
  ===============================================================================
  A:ALU-1#
```

Table 38: CRON schedule field descriptions

Label	Description
Schedule	The name of the schedule
Schedule owner	The name of the schedule owner
Description	The description of the schedule
Administrative status	Enabled — administrative status is enabled
	Disabled — administrative status is disabled
Operational status	Enabled — operational status is enabled
	Disabled — operational status is disabled
Script Policy	The name of the script policy
Script Policy Owner	The name of the script policy owner
Script	The name of the script
Script Owner	The name of the script owner
Script source location	The location of the scheduled script
Script results location	The location where the script results are sent
Schedule type	Periodic — displays a schedule that runs at a given interval
	Calendar — displays a schedule that runs based on a calendar
	Oneshot — displays a schedule that ran one time only
Interval	The interval between runs of an event

Label	Description
Repeat count	The number of times that the interval (periodic) schedule is run
Next scheduled run	The time for the next scheduled run
End time	The interval at which the schedule will end (periodic) or the date on which the schedule will end (calendar)
Weekday	The configured weekday
Month	The configured month
Day of month	The configured day of month
Hour	The configured hour
Minute	The configured minute
Number of schedule runs	The number of scheduled sessions
Last schedule run	The last scheduled session
Number of schedule failures	The number of scheduled sessions that failed to execute
Last schedule failure	The last scheduled session that failed to execute
Last failure time	The system time of the last failure

dhcp6

Syntax

dhcp6

Context

show>system

Description

This command displays system-wide DHCPv6 configuration information.

Output

The following output is an example of DHCPv6 configuration information, and Table 39: DHCPv6 configuration field descriptions describes the fields.

Output example

```
A:ALU-1# show system dhcp6
===============================================================================
DHCP6 system
```

```
================================================================================
Global NoAddrsAvail status  : esm-relay server
================================================================================
```

Table 39: DHCPv6 configuration field descriptions

Label	Description
Status	The system-wide status of DHCPv6 functionality

options

Syntax

   options

Context

   show>system>fp

Description

   This command displays information about forwarding path options.

   This command is only supported on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18.

Output

   The following output is an example of forwarding path information, and Table 40: Forwarding path field descriptions describes the fields.

   Output example

```
*A:7705:Dut-C# show system fp options
===============================================================================
System Forwarding Path Option Information
===============================================================================
Option                                 Admin State        Oper State
-------------------------------------------------------------------------------
vpls-high-scale                        Enabled            Disabled
-------------------------------------------------------------------------------
Reboot Required : Yes
```

Table 40: Forwarding path field descriptions

Label	Description
Option	The name of the forwarding path option
Admin State	The administrative status of the forwarding path option
Oper State	The operational status of the forwarding path option

Label	Description
Reboot Required	Indicates whether a system reboot is required for the forwarding path option to become operational

information

Syntax

   information

Context

   show>system

Description

   This command displays general system information including basic system, SNMP server, last boot and DNS client information.

Output

   The following output is an example of general system information, and Table 41: System information field descriptions describes the fields.

   Output example

```
A:7705:Dut-A# show system information

===============================================================================
System Information
===============================================================================
System Name           : A:7705:Dut-A
System Type           : 7705 SAR-8 v2
Chassis Topology      : Standalone
System Version        : B-0.0.I323
Crypto Module Version  :
 CPM: SARCM 3.0  DP: SARDCM 1.0
System Contact        : Fred Information Technology
System Location       : Bldg.1-floor 2-Room 201
System Coordinates    : N 85 58 23, W 34 56 12
System Active Slot    : A
System Up Time        : 1 days, 02:03:17.62 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f00006883ff000000
SNMP Engine Boots     : 58
SNMP Max Message Size : 1500
SNMP Admin State      : Enabled
SNMP Oper State       : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State       : OK

Tel/Tel6/SSH/FTP Admin : Enabled/Disabled/Enabled/Disabled
Tel/Tel6/SSH/FTP Oper  : Up/Down/Up/Down

BOF Source            : cf3:
Image Source          : primary
```

```
Config Source        : primary
Last Booted Config File: cf3:/config.cfg
Last Boot Cfg Version  : FRI APR 20 16:24:27 2007 UTC
Last Boot Config Header: # TiMOS-B-5.0.R3 both/hops NOKIA 7705 SAR #
                         Copyright (c) 2016 Nokia. All rights
                         reserved. # All use subject to applicable license
                         agreements. # Built on Wed Feb 13 19:45:00 EST 2016 by
                         builder in /rel5.0/R3/panos/main # Generated TUE
                         MAR 11 16:24:27 2016 UTC
Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-5.0.R3 both/hops NOKIA 7705 SAR #
                         Copyright (c) 2016 Nokia. All rights
                         reserved. # All use subject to applicable license
                         agreements. # Built on Wed Feb 13 19:45:00 EST 2016 by
                         builder in /rel5.0/R3/panos/main # Generated TUE
                         MAR 11 16:24:27 2016 UTC
Last Saved Config    : N/A
Time Last Saved      : N/A
Changes Since Last Save: Yes
User Last Modified   : admin
Time Last Modified   : 2016/03/19 10:03:09
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script        : N/A
Cfg-OK Script Status   : not used
Cfg-Fail Script      : N/A
Cfg-Fail Script Status : not used

Microwave S/W Package  : invalid

Management IP Addr     : 192.168.xxx.xxx/24
Primary DNS Server     : 192.168.xxx.xxx
Secondary DNS Server   : N/A
Tertiary DNS Server    : N/A
DNS Domain             : domain.com
DNS Resolve Preference : ipv4-only
BOF Static Routes      :
  To                   Next Hop
  192.xxx.0.0/16       192.xxx.1.1
ATM Location ID        : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ATM OAM Retry Up       : 2
ATM OAM Retry Down       : 4
ATM OAM Loopback Period  : 10

ICMP Vendor Enhancement: Disabled
Eth QinQ Untagged SAP  : False
===============================================================================
A:7705:Dut-A#
```

Table 41: System information field descriptions

Label	Description
System Name	The configured system name
System Type	The 7705 SAR chassis model
Chassis Topology	The chassis setup – always Standalone
System Version	The version of the installed software load
Crypto Module Version	The cryptographic module in the release

Label	Description
System Contact	A text string that describes the system contact information
System Location	A text string that describes the system location
System Coordinates	A text string that describes the system coordinates
System Active Slot	The active CSM slot
System Up Time	The time since the last boot
SNMP Port	The port number used by this node to receive SNMP request messages and to send replies
SNMP Engine ID	The SNMP engine ID to uniquely identify the SNMPv3 node
SNMP Engine Boots	The number of times that the SNMP engine has booted
SNMP Max Message Size:	The maximum SNMP packet size generated by this node
SNMP Admin State	Enabled — SNMP is administratively enabled and running
	Disabled — SNMP is administratively shut down and not running
SNMP Oper State	Enabled — SNMP is operationally enabled
	Disabled — SNMP is operationally disabled
SNMP Index Boot Status	Persistent — system indexes are saved between reboots
	Not Persistent — system indexes are not saved between reboots
Tel/Tel6/SSH/FTP Admin	The administrative state of the Telnet, Telnet IPv6, SSH, and FTP sessions
Tel/Tel6/SSH/FTP Oper	The operational state of the Telnet, Telnet IPv6, SSH, and FTP sessions
BOF Source	The location of the BOF
Image Source	Primary — Indicates that the directory location for runtime image file was loaded from the primary source
	Secondary — Indicates that the directory location for runtime image file was loaded from the secondary source
	Tertiary — Indicates that the directory location for runtime image file was loaded from the tertiary source
Config Source	Primary — Indicates that the directory location for configuration file was loaded from the primary source

Label	Description
	Secondary — Indicates that the directory location for configuration file was loaded from the secondary source
	Tertiary — Indicates that the directory location for configuration file was loaded from the tertiary source
Last Booted Config File	The URL and filename of the last loaded configuration file
Last Boot Cfg Version	The date and time of the last boot
Last Boot Config Header	The header information such as image version, date built, date generated
Last Boot Index Version	The version of the persistence index file read when this CSM card was last rebooted
Last Boot Index Header	The header of the persistence index file read when this CSM card was last rebooted
Last Saved Config	The location and filename of the last saved configuration file
Time Last Saved	The date and time of the last time configuration file was saved
Changes Since Last Save	Yes — There are unsaved configuration file changes
	No — There are no unsaved configuration file changes
User Last Modified	The username of the user who last modified the configuration file
Time Last Modified	The date and time of the last modification
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL — the location and name of the CLI script file executed following successful completion of the boot-up configuration file execution
	N/A — no CLI script file is executed
Cfg-OK Script Status	Successful/Failed — the results from the execution of the CLI script file specified in the Cfg-OK Script location
	Not used — no CLI script file was executed
Cfg-Fail Script	URL — the location and name of the CLI script file executed following a failed boot-up configuration file execution
	Not used — no CLI script file was executed

Label	Description
Cfg-Fail Script Status	Successful/Failed — the results from the execution of the CLI script file specified in the Cfg-Fail Script location
	Not used — no CLI script file was executed
Microwave S/W Package	N/A
Management IP Addr	The management IP address and mask
Primary DNS Server	The IP address of the primary DNS server
Secondary DNS Server	The IP address of the secondary DNS server
Tertiary DNS Server	The IP address of the tertiary DNS server
DNS Domain	The DNS domain name of the node
DNS Resolve Preference	N/A
BOF Static Routes	To — the static route destination
	Next Hop — the next hop IP address used to reach the destination
	Metric — displays the priority of this static route versus other static routes
	None — no static routes are configured
ATM Location ID	For ATM OAM loopbacks — the address of the network device referenced in the loopback request
ATM OAM Retry Up	N/A
Atm OAM Retry Down	N/A
ATM OAM Loopback Period	N/A
ICMP Vendor Enhancement	Enabled — inserts one-way timestamp in outbound SAA ICMP ping packets
	Disabled — one-way timestamping is not performed on outbound SAA ICMP ping packets
Eth QinQ untagged SAP	True: QinQ untagged SAPs are enabled
	False: QinQ untagged SAPs are disabled

lldp

Syntax

lldp neighbor

Context

show>system

Description

This command displays neighbor information for all configured ports without having to specify each individual port ID.

Output

The following output is an example of LLDP neighbor information, and Table 42: LLDP neighbor field descriptions describes the fields.

Output example

```
A:ALU-1# show system lldp neighbor
Link Layer Discovery Protocol (LLDP) System Information


===============================================================================
NB = nearest-bridge   NTPMR = nearest-non-tpmr   NC = nearest-customer
===============================================================================
Lcl Port        Scope Remote Chassis ID  Index  Remote Port      Remote Sys Name
-------------------------------------------------------------------------------
1/5/8           NB    38:52:1A:00:DC:01  2      1/8/8, 10/100/* 7705:Dut-C
1/5/8           NTPMR BC:52:B4:2B:D0:7D  3      1/1/1, 10/100/* 7705:Dut-F
1/5/8           NC    BC:52:B4:2B:D0:7D  4      1/1/1, 10/100/* 7705:Dut-F
1/5/8           NTPMR 38:52:1A:00:E0:01  5      1/4/3, 10/100/* 7705:Dut-A
1/5/8           NC    38:52:1A:00:E0:01  6      1/4/3, 10/100/* 7705:Dut-A
1/4/3           NTPMR 38:52:1A:00:E0:01  7      1/5/8, 10/100/* 7705:Dut-A
1/4/3           NC    38:52:1A:00:E0:01  8      1/5/8, 10/100/* 7705:Dut-A
1/4/3           NTPMR BC:52:B4:2B:D0:7D  9      1/1/1, 10/100/* 7705:Dut-F
1/4/3           NC    BC:52:B4:2B:D0:7D  10     1/1/1, 10/100/* 7705:Dut-F
1/4/3           NB    00:25:BA:17:2A:42  15     BA              7705:Dut-B
===============================================================================
* indicates that the corresponding row element may have been truncated.
Number of neighbors : 10
A:ALU-1#
```

Table 42: LLDP neighbor field descriptions

Label	Description
Lcl Port	The physical port ID of the local port in *slot/mda/port* format
Scope	The scope of LLDP supported: NB (nearest bridge), NTPMR (nearest non-two-port MAC relay bridge), or NC (nearest customer bridge)
Remote Chassis ID	The MAC address of the chassis containing the Ethernet port that sent the LLDPDU

Label	Description
Index	The LLDP remote peer index
Remote Port	The physical port ID of the remote port in *slot/mda/port* format and a port description (based on ifDescr from RFC 2863 - IF MIB)
	If a port-description TLV is received, displays the ifDescr object for the interface – a text string containing information about the interface
	If a port-description TLV is not received or the value is null, displays the ifindex for the interface
	(* indicates that the output has been truncated)
Remote Sys Name	The name of the remote chassis

load-balancing-alg

Syntax

load-balancing-alg [**detail**]

Context

show>system

Description

This command displays the system load-balancing settings.

Parameters

detail

displays detailed information for load-balancing algorithms

Output

The following output is an example of system load-balancing algorithm information, and Table 43: System load-balancing algorithm field descriptions describes the fields.

Output example

```
*A:Sar18 Dut-B>show>system# load-balancing-alg
===============================================================================
System-wide Load Balancing Algorithms
===============================================================================
L4 Load Balancing                      : exclude-L4
LSR Load Balancing                     :
    Hashing Algorithm                  : lbl-only
    Hashing Treatment                  : profile-1
    Use Ingress Port                   : disabled
System IP Load Balancing               : enabled
===============================================================================
```

```
*A:Sar18 Dut-B>show>system#
```

Table 43: System load-balancing algorithm field descriptions

Label	Description
System-wide Load Balancing Algorithms	
L4 Load Balancing	The configured setting for **l4-load-balancing**
LSR Load Balancing	The configured settings for **lsr-load-balancing**, including: • Hashing Algorithm The configured hashing algorithm: lbl-only, lbl-ip, or lbl-ip-l4-teid • Hashing Treatment The configured label stack profile: profile-1, profile-2, or profile-3 • Use Ingress Port Specifies whether the ingress port at the LSR is used
System IP Load Balancing	Specifies whether the system IP address is used in the load-balancing calculation

memory-pools

Syntax

memory-pools

Context

show>system

Description

This command displays system memory status.

Output

The following output is an example of system memory information, and Table 44: Memory pool field descriptions describes the fields.

Output example

```
A:ALU-1# show system memory-pools

===============================================================================
Memory Pools
===============================================================================
Name               Max Allowed    Current Size    Max So Far        In Use
-------------------------------------------------------------------------------
```

```
System               No limit        308,145,416        316,100,296        300,830,200
Icc              16,777,216          2,097,152          2,097,152            773,920
RTM/Policies         No limit          2,097,152          2,097,152          1,027,792
OSPF                 No limit          1,048,576          1,048,576            437,904
MPLS/RSVP            No limit         21,145,848         21,145,848         19,562,376
LDP                  No limit          1,048,576          1,048,576            224,848
IS-IS                No limit                  0                  0                  0
RIP                  No limit                  0                  0                  0
VRRP                 No limit          1,048,576          1,048,576              1,144
BGP                  No limit          2,097,152          2,097,152          1,176,560
Services             No limit          5,685,504          5,685,504          3,884,512
IOM                  No limit        249,068,424        249,068,424        245,119,136
SIM                  No limit          1,048,576          1,048,576            129,808
IP Stack             No limit          4,295,184          4,295,184          3,189,048
MBUF                 No limit          1,048,576          1,048,576            151,520
IGMP/MLD Snpg        No limit          1,048,576          1,048,576             71,192
TLS MFIB             No limit          1,048,576          1,048,576          1,027,312
WEB Redirect     16,777,216                  0                  0                  0
BFD                  No limit          1,048,576          1,048,576            828,448
MCPATH               No limit          1,048,576          1,048,576                472
-------------------------------------------------------------------------------
Current Total Size :    604,069,016 bytes
Total In Use       :    578,436,192 bytes
Available Memory   :     78,909,496 bytes
===============================================================================
*A:ALU-1#
```

Table 44: Memory pool field descriptions

Label	Description
Name	The name of the system or process
Max Allowed	Integer — the maximum allocated memory size
	No Limit — no size limit
Current Size	The current size of the memory pool
Max So Far	The largest amount of memory pool used
In Use	The current amount of the memory pool currently in use
Current Total Size	The sum of the Current Size column
Total In Use	The sum of the In Use column
Available Memory	The amount of available memory

ntp

Syntax

ntp [{**peers** | **peer** *peer-address* } | {**servers** | **server** *server-address*} | [**all**]] [**detail**]

Context

show>system

Description

This command displays NTP protocol configuration and state information.

Parameters

peers

displays information about the remote systems that are configured as NTP peers

peer-address

displays information about the specified NTP peer

servers

displays information about sources that are configured as NTP servers

server-address

displays information about the specified node that is configured as an NTP server

all

displays a summary of all configured NTP peer and server information

detail

displays detailed NTP configuration information

Output

The following output is an example of NTP information, and Table 45: System NTP field descriptions describes the fields.

Output example

```
A:Sar18 Dut-B# show system ntp
===============================================================================
NTP Status
===============================================================================
Configured        : Yes              Stratum             : 4
Admin Status      : up               Oper Status         : up
Server Enabled    : Yes              Server Authenticate : Yes
Clock Source      : 135.121.107.98
Auth Check        : Yes
MDA Timestamp     : No
Current Date & Time: 2021/03/22 17:28:09 UTC
===============================================================================


*A:Sar18 Dut-B# show system ntp all
===============================================================================
NTP Status
===============================================================================
Configured        : Yes              Stratum             : 4
Admin Status      : up               Oper Status         : up
Server Enabled    : Yes              Server Authenticate : Yes
Clock Source      : 135.121.107.98
Auth Check        : Yes
MDA Timestamp     : No
Current Date & Time: 2021/03/22 17:30:00 UTC
===============================================================================
```

```
===============================================================================
NTP Active Associations
===============================================================================
State                   Reference ID   St Type  A  Poll Reach     Offset(ms)
    Remote
-------------------------------------------------------------------------------
chosen                  138.120.210.186 3  srvr  -  64   YYYYYYYY  0.124
    135.121.107.98
reject                  INIT           -  actpr n  64   ........  0.000
    135.121.107.100
===============================================================================
===============================================================================
NTP Clients
===============================================================================
vRouter                                              Time Last Request Rx
    Address
-------------------------------------------------------------------------------
===============================================================================
```

```
*A:Sar18 Dut-B# show system ntp detail
===============================================================================
NTP Status
===============================================================================
Configured        : Yes              Stratum            : 4
Admin Status      : up               Oper Status        : up
Server Enabled    : Yes              Server Authenticate  : Yes
Clock Source      : 135.121.107.98
Auth Check        : Yes
MDA Timestamp     : No
Auth Errors       : 0                Auth Errors Ignored  : 0
Auth Key Id Errors : 0               Auth Key Type Errors : 0
Current Date & Time: 2021/03/22 17:34:46 UTC
===============================================================================
===============================================================================
NTP Configured Broadcast/Multicast Interfaces
===============================================================================
vRouter         Interface         Address           Type    Auth    Poll
-------------------------------------------------------------------------------
===============================================================================
```

```
*A:Sar18 Dut-B# show system ntp detail all
===============================================================================
NTP Status
===============================================================================
Configured        : Yes              Stratum            : 4
Admin Status      : up               Oper Status        : up
Server Enabled    : Yes              Server Authenticate  : Yes
Clock Source      : 135.121.107.98
Auth Check        : Yes
MDA Timestamp     : No
Auth Errors       : 0                Auth Errors Ignored  : 0
Auth Key Id Errors : 0               Auth Key Type Errors : 0
Current Date & Time: 2021/03/22 17:36:45 UTC
===============================================================================
===============================================================================
NTP Configured Broadcast/Multicast Interfaces
===============================================================================
vRouter         Interface         Address           Type    Auth    Poll
-------------------------------------------------------------------------------
===============================================================================
===============================================================================
NTP Active Associations
```

```
===============================================================================
State                    Reference ID    St Type  A  Poll Reach    Offset(ms)
    Remote
-------------------------------------------------------------------------------
chosen                   138.120.210.186 3  srvr  -  64   YYYYYYYY  0.105
    135.121.107.98
reject                   INIT            -  actpr n  64   ........  0.000
    135.121.107.100
===============================================================================
===============================================================================
NTP Clients
===============================================================================
vRouter                                           Time Last Request Rx
    Address
-------------------------------------------------------------------------------
===============================================================================


*A:Sar18 Dut-B# show system ntp peer 135.121.107.100 detail
===============================================================================
NTP Peer
===============================================================================
State                    Reference ID    St Type  A  Poll Reach    Offset(ms)
    Remote
-------------------------------------------------------------------------------
reject                   INIT            -  actpr n  64   ........  0.000
    135.121.107.100
===============================================================================


*A:7705:Dut-C# show system ntp peer 3333:50:1::4
===============================================================================
NTP Peer
===============================================================================
State                    Reference ID    St Type  A  Poll Reach    Offset(ms)
    Remote
-------------------------------------------------------------------------------
outlyer                  138.120.193.198 2  actpr y  8    Y.YYYYY.  -0.858
    3333:50:1::4
===============================================================================
*A:7705:Dut-C#
```

Table 45: System NTP field descriptions

Label	Description
NTP Status	
Configured	Indicates whether NTP is enabled: yes or no
Stratum	The stratum level of this node
Admin Status	Indicates the administrative state: up or down
Oper Status	Indicates the operational status: up or down
Server Enabled	Indicates whether the NTP server is enabled on this node: yes or no

Label	Description
Server Authenticate	Indicates whether NTP server authentication is required: yes or no
Clock Source	The IP address of the node acting as the clock source
Auth Check	Indicates whether an authentication check is required: yes or no
MDA Timestamp	Indicates whether MDA timestamping is enabled for NTP: yes or no
Current Date & Time	The current date and time
Auth Errors	Number of authentication errors
Auth Errors Ignored	Number of authentication errors ignored
Auth Key Id Errors	Number of authentication key identification errors
Auth Key Type Errors	Number of authentication key type errors
NTP Configured Broadcast/Multicast Interfaces	
vRouter	The router instance containing the interface
Interface	The interface configured in NTP
Address	The address used for transmitted messages
Type	The interface type: • bcast — broadcast interface • mcast — multicast interface • bclnt — broadcast client • svr — server • actpr — active peer • paspr — passive peer
Auth	Indicates whether authentication is in use
Poll	The current poll interval used on the interface
NTP Active Associations	
State	The state of the peers acting as time servers: • Reject The peer is rejected and will not be used for synchronization. Rejection reasons could be that the peer is unreachable, the peer is synchronized to this local server so synchronizing with it would create a synchronization loop, or the synchronization distance is too large. This is the normal startup state.

Label	Description
	• Invalid The peer is not maintaining an accurate clock. This peer will not be used for synchronization. • Excess The peer's synchronization distance is greater than 10 other peers. This peer will not be used for synchronization. • Outlyer The peer is discarded as an outlier. This peer will not be used for synchronization. • Candidate The peer is accepted as a possible source of synchronization • Selected The peer is an acceptable source of synchronization, but its synchronization distance is greater than six other peers • Chosen The peer is chosen as the source of synchronization • ChosenPPS The peer is chosen as the source of synchronization, but the actual synchronization is occurring from a pulse-per-second (PPS) signal
Remote	The IP address of the remote NTP server or peer with which this local host is exchanging NTP packets
Reference ID	When the Stratum level is between 0 and 15, this field shows the IP address of the remote NTP server or peer with which the local server or peer is exchanging NTP packets. For reference clocks, this field shows the identification assigned to the clock, such as ".GPS." For an NTP server or peer, if the client has not yet synchronized to a server/peer, the status cannot be determined and the following codes are displayed: ACST — the association belongs to a unicast server AUTH — server authentication failed. Please wait while the association is restarted. AUTO — autokey sequence failed. Please wait while the association is restarted. BCST — the association belongs to a broadcast server CRPT — cryptographic authentication or identification failed. The details should be in the system log file or the cryptostats statistics file, if configured. No further messages will be sent to the server. DENY — access denied by remote server. No further messages will be sent to the server.

Label	Description
	DROP — lost peer in symmetric mode. Please wait while the association is restarted.
	RSTR — access denied due to local policy. No further messages will be sent to the server.
	INIT — the association has not yet synchronized for the first time
	INIT — the system clock has not yet synchronized for the first time
	STEP — a step change in system time has occurred, but the system clock has not yet resynchronized
St	The Stratum level of this node
Type	The peer type: • bcast — broadcast interface • mcast — multicast interface • bclnt — broadcast client • svr — server • actpr — active peer • paspr — passive peer
A	Authentication
Poll	Polling interval in seconds
Reach	Yes — the NTP peer or server has been reached at least once in the last eight polls
	No — the NTP peer or server has not been reached at least once in the last eight polls
Offset (ms)	The difference between the local and remote UTC time, in milliseconds
NTP Clients	
vRouter	The router instance containing the interface
Address	The address used for the transmitted messages
Time last Request Rx	The time at which the last request was received from the client

poe

Syntax

poe

Context

show>system

Description

This command shows a summary of the PoE status of each PoE capable port in the system.

Output

The following output is an example of PoE status information, and Table 46: System PoE status field descriptions describes the fields.

Output example

```
A:# show system poe
===============================================================================
PoE Information
===============================================================================
PoE Maximum Power Budget       : 83.8 watts
PoE Power Committed            : 65.0 watts
PoE Power Available            : 18.8 watts
PoE Power In Use               : 0.0 watts


===============================================================================
PoE Port Information
===============================================================================
Interface    PoE            PoE            Maximum        Power
             Mode           Detection      Power          In Use
-------------------------------------------------------------------------------
1/1/5        Standard       Searching      15.4 watts     0.0 watts
1/1/6        Disabled        Disabled       0.0 watts     0.0 watts
1/1/7            Plus       Searching      34.2 watts     0.0 watts
1/1/8        Standard       Searching      15.4 watts     0.0 watts
===============================================================================
```

Table 46: System PoE status field descriptions

Label	Description
PoE Maximum Power Budget	The maximum PoE power budget available for the system
PoE Power Committed	The total PoE power that has been configured on all PoE or PoE+ ports on the system
PoE Power Available	The amount of PoE power available to be configured on additional PoE or PoE+ ports on the system
PoE Power In Use	The total PoE power currently being used by all PoE or PoE+ configured ports on the system
PoE Mode	Indicates whether the port is using standard PoE or PoE+ If the PoE function is turned off, the mode is Disabled
PoE Detection	Indicates the detection state of the PoE port
Maximum Power	The maximum PoE power available on the port

© 2024 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Label	Description
Power in Use	The amount of PoE power currently being used on the port

ptp

Syntax

ptp

ptp timestamp-stats

Context

show>system

Description

This command displays general PTP information and PTP timestamp information.

Parameters

timestamp-stats

displays port statistics for packets with timestamp updated fields

Output

The following outputs are examples of PTP information:

• system PTP information (Output example, Table 47: System PTP field descriptions)

• PTP timestamp information (Output example, Table 48: System PTP timestamp field descriptions)

Output example

```
*A:# show system ptp
===============================================================================
Clk   Source IP       Clock-type    MDA  Admin  PTP Clock Id      Node Time-Ref-
Idx                                      State                    Ref  Priority
===============================================================================
csm n/a               ordin/slave   n/a  down   d665fffffe000000  -    -
2                     ordin/slave   1/1  up     d665fffffe000002       -
===============================================================================
```

Table 47: System PTP field descriptions

Label	Description
Clk Idx	The clock identifier, either 1 to 16 or csm
Source IP	The IP address of the source interface
Clock-type	The clock type: ordin/slave, ordin/master, boundary, transparent

Label	Description
MDA	The adapter card slot that performs the IEEE 1588v2 clock recovery
Admin State	up – the local PTP clock is administratively enabled down – the local PTP clock is administratively disabled
PTP Clock Id	A unique 64-bit number assigned to the clock
Node Ref	Timing reference: ref1 or ref2; applicable if the clock is a source of synchronization timing for the node
Time-Ref-Priority	The priority value of the clock, used to determine which clock provides timing for the network

Output example

```
A:# show system ptp timestamp-stats
===============================================================================
 PTP Port Timestamp Summary
-------------------------------------------------------------------------------
Phys    In/   Sync          Delay Req          Follow-Up
Port    Out   Pkt           Pkt                Pkt
===============================================================================
1/1/1   in    0             19529              -
        out   19558         0                  19558
1/3/1   in    0             4763373            -
        out   4763374       0                  4763374
===============================================================================
*A:#
```

Table 48: System PTP timestamp field descriptions

Label	Description
Phys Port	The physical port identifier
In/Out	The direction of the packet counts
Sync Pkt	The number of ingress or egress synchronization packets
Delay Req Pkt	The number of ingress or egress delay request packets
Follow-Up Pkt	The number of egress follow-up packets

clock

Syntax

clock *clock-id*

clock *clock-id* **bmc**

clock *clock-id* **detail**

clock *clock-id* **standby**

clock *clock-id* **statistics**

clock *clock-id* **summary**

clock *clock-id* **unicast**

Context

show>system>ptp

Description

This command displays PTP clock information.

Parameters

clock-id

specifies the clock ID of this PTP instance

> **Values**   1 to 16 for PTP clocks that use IPv4 encapsulation
>
> **csm** for a PTP clock that uses Ethernet encapsulation

bmc

displays information about the BTCA configured for each PTP peer. This command only applies when the *clock-id* parameter value is 1 to 16.

detail

displays detailed information about the specified PTP clock. This command only applies when the *clock-id* parameter value is 1 to 16.

standby

displays PTP information about the standby CSM. This command only applies when the *clock-id* parameter is defined as **csm**.

statistics

displays statistics information. This command only applies when the *clock-id* parameter is defined as **csm**.

summary

displays summary information. This command only applies when the *clock-id* parameter value is 1 to 16.

unicast

displays IP unicast negotiation information. This command only applies when the *clock-id* parameter value is 1 to 16.

Output

The following outputs are examples of PTP clock information:

- PTP clock CSM summary information (Output example, Table 49: System PTP clock CSM field descriptions)

- PTP clock CSM statistics information (Output example, Table 50: System PTP clock CSM statistics field descriptions)
- PTP clock summary information (Output example, Table 51: System PTP clock summary field descriptions)
- PTP clock information (Output example, Table 52: System PTP clock field descriptions)

Output example

```
A:# show system# ptp clock csm
===============================================================================
IEEE 1588/PTP Clock Information
===============================================================================
-------------------------------------------------------------------------------
Local Clock
-------------------------------------------------------------------------------
Clock Type        : ordinary,slave    PTP Profile        : IEEE 1588-2008
Domain            : 0                 Network Type       : sdh
Admin State       : down              Oper State         : down
Announce Interval : 1 pkt/2 s         Announce Rx Timeout: 3 intervals
Clock Id          : 4cc94ffffe737123  Clock Class        : 255 (slave-only)
Clock Accuracy    : unknown           Clock Variance     : ffff (not computed)
Clock Priority1   : 128               Clock Priority2    : 128
Steps Removed: 6
PTP Port State    : disabled          Last Changed       : 10/28/2015 18:48:31
PTP Recovery State: disabled
Frequency Offset  : n/a
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
PTP Time Recovery
-------------------------------------------------------------------------------
Time Recovery Sta*: locked            Last Changed       : 2023/11/08 14:47:44
Last Offset From *: -4 ns             Last Calc          : 2023/11/08 14:55:17
Last Mean Path De*: +10 ns            Last Calc          : 2023/11/08 14:55:17
Last Adjustment   : 0 ns              Last Calc          : 2023/11/08 14:55:16
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
Time Information
-------------------------------------------------------------------------------
Timescale         : Arbitrary
Current Time      : 2015/11/02 15:51:44.8 (ARB)
Frequency Traceable : no
Time Traceable    : no
Time Source       : internal oscillator
===============================================================================
A:# show system#
```

Table 49: System PTP clock CSM field descriptions

Label	Description
Local Clock	
Clock Type	The local PTP clock type, one of: ordinary master, ordinary slave, boundary, or transparent-e2e
PTP Profile	The PTP profile: ieee-1588, itu-telecom-freq, g8275dot1-2014, g8275dot2-2016, iec-61850-9-3-2016, or c37dot238-2017

Label	Description
Domain	The PTP device domain
Network Type	Indicates whether SONET or SDH values are being used for encoding synchronous status messages
Admin State	up – the local PTP clock is administratively enabled
	down – the local clock is administratively shut down and not running
Oper State	Up – the local clock is operationally enabled and running
	Down – the local clock is operationally disabled and not running
Announce Interval	The message interval used for Announce messages
Announce Rx Timeout	The number of Announce timeouts that need to occur on a PTP timeReceiver port or boundary clock port in timeReceiver mode before communication messages with a timeTransmitter clock are deemed lost and the timeTransmitter clock is considered not available
Clock Id	A unique 64-bit number assigned to the clock
Clock Class	The local clock class
Clock Accuracy	The local clock accuracy designation
Clock Variance	The local clock variance
Clock Priority1	The first priority value of the local clock, used by the BTCA to determine which clock should provide timing for the network
Clock Priority2	The second priority value of the local clock. This value is used by the BTCA to determine which clock should provide timing for the network.
Steps Removed	The number of hops from the PTP grandmaster clock. This value is used by the BTCA to determine which clock should provide timing to the network when the profile is set to **g8275dot1-2014** or **g8275dot2-2016**.
PTP Port State	The PTP port state, one of: disabled, listening, slave, master, passive, or faulty
Last Changed	The time the PTP port state last changed
PTP Recovery State	The clock recovery state, one of: disabled, initial, acquiring, phase-tracking, or locked
Frequency Offset	The frequency offset of the PTP clock in parts per billion
PTP Time Recovery	

Label	Description
Time Recovery State	The state of the time recovery algorithm: • acquiring — the algorithm is active but is not in a locked or holdover state • locked — the algorithm is generating time adjustments within the locked performance range • holdover — the algorithm has not generated time adjustments for a period of time
Last Changed	The date and time when the Time Recovery State field last changed
Last Offset From Master	The offsetFromMaster value, in nanoseconds, calculated from the last packet exchange with the parent clock
Last Calc	The date and time when the field was last calculated
Last Mean Path Delay	The meanPathDelay value, in nanoseconds, calculated from the last packet exchange with the parent clock
Last Adjustment	The change to the local time scale, in nanoseconds, that was last generated by the time recovery algorithm
Time Information	
Timescale	The PTP timescale flag sent in the 1588 Announce message
Current Time	The last date and time recovered by the PTP time recovery algorithm
Frequency Traceable	The frequency-traceable flag sent in the 1588 Announce message
Time Source	The time-source parameter sent in the 1588 Announce message

Output example

```
*A:SAR8-39-2>config>system>ptp>clock># show system ptp clock csm statistics
===============================================================================
IEEE 1588/PTP Packet Statistics
===============================================================================
                                                          Input      Output
-------------------------------------------------------------------------------
PTP Packets                                               101358     101358
  Announce                                                     0          0
  Sync                                                         0          0
  Follow Up                                                    0          0
  Delay Request                                                0          0
  Delay Response                                               0          0
  Peer Delay Request                                      101326         32
  Peer Delay Response                                         32     101326
  Peer Delay Response Follow Up                               0          0
  Signaling                                                    0          0
  Other                                                       0          0
```

```
Discards                                            4457103         0
  Bad PTP domain                                    4457103         0
  Alternate Master                                        0         0
  Out Of Sequence                                        0         0
  Other                                                  0         0
TLVs
  IEEE C37.238                                           0         0
  Alternate Time Offset Indicator (ATOI)                 0         0
  Discarded (Unknown or Error)                           0         0
===============================================================================
===============================================================================
IEEE 1588/PTP Frequency Recovery State Statistics
===============================================================================
State                                                          Seconds
-------------------------------------------------------------------------------
Initial                                                        6181014
Acquiring                                                            0
Phase-Tracking                                                      0
Locked                                                             0
Hold-over                                                          0
===============================================================================
===============================================================================
IEEE 1588/PTP Event Statistics
===============================================================================
Event                                           Sync Flow Delay Flow
-------------------------------------------------------------------------------
Packet Loss                                            0         0
Excessive Packet Loss                                  0         0
Excessive Phase Shift Detected                         0         0
Too Much Packet Delay Variation                        0         0
===============================================================================
===============================================================================
IEEE 1588/PTP Message Rates Per Second
===============================================================================
                                                      Ethernet
Packet Type                                      Input    Output
-------------------------------------------------------------------------------
Announce                                              0         0
Sync                                                  0         0
Follow Up                                             0         0
Delay Request                                         0         0
Delay Response                                        0         0
Peer Delay Request                                    1         1
Peer Delay Response                                   1         1
Peer Delay Response Follow Up                         0         0
Other                                                 0         0
-------------------------------------------------------------------------------
Total                                                 2         2
===============================================================================
```

Table 50: System PTP clock CSM statistics field descriptions

Label	Description
IEEE 1588/PTP Packet Statistics	
PTP Packets	The total number of input or output PTP packets
Announce	The number of input or output Announce packets
Sync	The number of input or output synchronization packets

Label	Description
Follow Up	The number of input or output follow-up packets
Delay Request	The number of input or output delay request packets
Delay Response	The number of input or output delay response packets
Peer Delay Request	The number of input or output peer delay request packets
Peer Delay Response	The number of input or output peer delay response packets
Peer Delay Response Follow Up	The number of input or output peer delay response follow-up packets
Signaling	The number of input or output signaling packets
Other	The number of other input or output packets
Discards	The total number of discarded packets
Bad PTP domain	The number of input or output packets discarded with bad PTP domain
Alternate Master	The number of input or output packets discarded with alternate master
Out of Sequence	The number of input or output packets discarded as out of sequence
Other	The number of other input or output discarded packets
TLVs	The TLVs sent and received
IEEE C37.238	The number of IEEE C37.238 TLVs This field is visible but the rate is not displayed to the operator
Alternate Time Offset Indicator (ATOI)	The number of ATOI TLVs This field is visible but the rate is not displayed to the operator
Discard (Unknown or Error)	The number of discarded TLVs This field is visible but the rate is not displayed to the operator
IEEE 1588/PTP Frequency Recovery State Statistics	
State	The following algorithm state statistics (in seconds) are provided for the CSM clock: • Initial • Acquiring • Phase-Tracking • Locked

Label	Description
	• Hold-over
IEEE 1588/PTP Event Statistics	
Event	The following algorithm event statistics (in seconds) are provided for the CSM clock: • Packet Loss • Excessive Packet Loss • Excessive Phase Shift Detected • Too Much Packet Delay Variation
IEEE 1588/PTP Message Rates Per Second	
Packet Type	The following algorithm message rates per second are provided for the CSM clock: • Announce • Sync • Follow Up • Delay Request • Delay Response • Peer Delay Request • Peer Delay Response • Peer Delay Response Follow Up • Other

Output example

```
A:# show system ptp clock 2 summary
===============================================================================
-------------------------------------------------------------------------------
PtpPort/Peer        : 1/1
IP Address          : 10.10.10.10
Static/Dynamic      : Static
PTP Port State      : initializing
                                                        Rx          Tx
-------------------------------------------------------------------------------
Anno                                                    623         0
Sync                                                    82990       0
Follow-Up                                               82990       -
DelayRequest                                            82998       82998
DelayResponse                                           82998       82998
===============================================================================
===============================================================================
Unicast Negotiation Summary
-------------------------------------------------------------------------------
Prt/ Peer IP        In/ Anno   Sync   Delay  Anno       Sync       Delay
Peer                Out Lease  Lease  Lease  Rate       Rate       Rate
                        (sec)  (sec)  (sec)  (pkt/s)    (pkt/s)    (pkt/s)
===============================================================================
```

```
1/1  10.222.222.10    in  174     182     182    1 pkt/2 s  64 pkt/s   64 pkt/s
                      out -       -       -      -          -          -
1/2                       -   -   -       -      -          -          -
                      out -       -       -      -          -          -
===============================================================================
===============================================================================
Best Master Clock Summary
-------------------------------------------------------------------------------
Prt/ Peer IP        Slave Pri1 GM    GM    GM     Pri2 GM ClockId       Step
Peer                        Clk   Clk   Clk                             Rem
                            Cls   Acc   Var
===============================================================================
1/1  10.222.222.10  yes   128   6     3e3    25600  128  4041424344454637 1
1/2                 -     -     -     -      -      -    -                 -
===============================================================================
```

Output example (boundary clock)

```
A:# show system ptp clock 1 summary
===============================================================================
Prt/ Peer IP        Slave Port   Dyn/ In/ Anno      Sync        Delay
Peer                      State  Stat Out                       Req/Resp
===============================================================================
1/1  192.253.252.10  no   master  sta in  7         0           0
                                  sta out 770       0           0
2/1  192.254.254.10  no   master  sta in  0         0           103052
                                  sta out 773       103054      103052
3/1  192.253.252.11       no   master  sta in  0         0           0
                                  sta out 0         0           0
4/1                  no   initia* sta in  0         0           0
                                  sta out 0         0           0
5/1                  no   initia* sta in  0         0           0
                                  sta out 0         0           0
6/1                  no   initia* sta in  0         0           0
                                  sta out 0         0           0
7/1                  no   initia* sta in  0         0           0
                                  sta out 0         0           0
8/1                  no   master  sta in  0         0           0
                                  sta out 0         0           0
9/1  192.168.254.12   yes  slave   sta in  823       105272      105271
                                  sta out 0         0           105271
10/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
11/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
12/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
13/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
14/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
15/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
...

50/1                 no   initia* sta in  0         0           0
                                  sta out 0         0           0
===============================================================================
Prt/ Peer IP        In/ Anno  Sync   Delay  Anno      Sync        Delay
Peer                Out Lease Lease  Lease  Rate      Rate        Rate
                        (sec) (sec)  (sec)  (pkt/s)   (pkt/s)     (pkt/s)
===============================================================================
1/1  192.253.254.8  in  166   0      0      1 pkt/2 s -           -
```

```
                  out 228    -       -        1 pkt/2 s  -           -
2/1  192.254.254.9  in  1      0       0        -          -           -
                  out 231    235     235      1 pkt/2 s  64 pkt/ s  64 pkt/s
3/1  192.253.252.11        in  1      0       0        -          -           -
                  out -      -       -        -          -           -
4/1               -    -    -       -        -          -           -
                  out -      -       -        -          -           -
5/1               -    -    -       -        -          -           -
                  out -      -       -        -          -           -
6/1               -    -    -       -        -          -           -
                  out -      -       -        -          -           -
7/1               -    -    -       -        -          -           -
                  out -      -       -        -          -           -
8/1               -    -    -       -        -          -           -
                  out -      -       -        -          -           -
9/1  192.168.255.11   in  102    106     106      1 pkt/2 s  64 pkt/s   64 pkt/s
                  out -      -       -        -          -           -
10/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
11/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
12/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
13/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
14/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
15/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
...

50/1              -    -    -       -        -          -           -
                  out -      -       -        -          -           -
===========================================================================
Prt/ Peer IP       Slave Pri1 GM     GM      GM      Pri2 GM ClockId       Step
Peer                         Clk    Clk     Clk                           Rem
                             Cls    Acc     Var
===========================================================================
1/1  192.253.2.10  no    128  13     254     65535   128  002105fffe6da9b7 0
2/1  192.254.2.10  no    -    -      -       -       -    -                -
3/1  192.255.2.10        no   -      -       -       -    -         -              -
4/1                -     -    -      -       -       -    -                -
5/1                -     -    -      -       -       -    -                -
6/1                -     -    -      -       -       -    -                -
7/1                -     -    -      -       -       -    -                -
8/1                -     -    -      -       -       -    -                -
9/1  192.168.2.11  yes   128  6      33      25600   128  4041424344454637 0
10/1               -     -    -      -       -       -    -                -
11/1               -     -    -      -       -       -    -                -
12/1               -     -    -      -       -       -    -                -
13/1               -     -    -      -       -       -    -                -
14/1               -     -    -      -       -       -    -                -
15/1               -     -    -      -       -       -    -                -
...

50/1               -     -    -      -       -       -    -                -
```

Table 51: System PTP clock summary field descriptions

Label	Description
PtpPort/Peer Prt/Peer	The PTP port and peer ID as configured in the *config>system>ptp>clock* context
IP Address Peer IP	The IP address of the PTP peer
Static/Dynamic Dyn/Stat	Indicates if the peer is statically configured or dynamically requested
PTP Port State Port State	The PTP port state: initializing, listening, uncalibrated, slave, master, or passive
Slave	Indicates whether the clock is in a timeReceiver state
Rx/Tx In/Out	The direction of the packet counts
Anno	The number of ingress or egress Announce packets
Sync	The number of ingress or egress synchronization packets
Follow-Up	The number of ingress follow-up packets
DelayRequest	The number of ingress or egress delay request packets
DelayResponse	The number of ingress or egress delay response packets
Anno Lease	The Announce time remaining in the unicast session. The peer must re-request Announce before this expires or the peer communication will be canceled.
Sync Lease	The synchronization time remaining in the unicast session. The peer must re-request synchronization before this expires or the peer communication will be canceled.
Delay Lease	The delay time remaining in the unicast session. The peer must re-request delay before this expires or the peer communication will be canceled.
Anno Rate	The rate of Announce packets to or from the peer
Sync Rate	The rate of synchronization packets to or from the peer
Delay Rate	The rate of delay packets to or from the peer
Pri1	The grandmaster clock priority1 designation
GM Clk Cls	The grandmaster clock class designation

Label	Description
GM Clk Acc	The grandmaster clock accuracy designation
GM Clk Var	The grandmaster clock scaled log variance, in decimal format
Pri2	The grandmaster clock priority2 designation
GM ClockId	The grandmaster clock identification
Step Rem	The number of boundary clocks between the peer and the grandmaster

Output example

```
A:7705:Dut-I# show system ptp clock 2
===============================================================================
IEEE1588 PTP Clock Information
===============================================================================
-------------------------------------------------------------------------------
Local Clock
-------------------------------------------------------------------------------
Clock Type           : ordinary,slave   Admin State          : up
Source Interface     : system           Clock MDA            : 1/1
PTP Profile          : g8275dot2-2016   Domain               : 44
Clock ID             : d665fffffe000002 Clock Class          : 255
Clock Accuracy       : unknown(254)     Clock Variance       : not computed
Clock Priority1      : 128              Clock Priority2      : 255
Clock Local-priority : 222
Steps Removed: 1
Use Node Time        : no               Dynamic Peers        : not allowed
Admin Freq-source    : ptp              Oper Freq-source     : ptp
Tx While Sync Uncert*: true             Sync Certainty State : uncertain
Two-Step             : unknown
-------------------------------------------------------------------------------
Parent Clock
-------------------------------------------------------------------------------
Parent Clock ID      : 34aa99fffeea4250 Parent Port Number   : 3
GM Clock Id          : 702526fffea852a2 GM Clock Class       : 6
GM Clock Accuracy    : 100ns            GM Clock Variance    : 20061
GM Clock Priority1   : 128              GM Clock Priority2   : 128
Rx Sync Certainty    : uncertain


-------------------------------------------------------------------------------
PTP Time Recovery
-------------------------------------------------------------------------------
Time Recovery State  : locked           Last Changed      : 2023/11/08 10:51:58
Last Offset From Mas*: -20 ns           Last Calc         : 2023/11/08 10:51:58
Last Mean Path Delay : -10 ns           Last Calc         : 2023/11/08 10:51:58
Last Adjustment      : -30 ns           Last Calc         : 2023/11/08 12:05:34
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
Time Information
-------------------------------------------------------------------------------
Timescale            : PTP
Recovered Date/Time  : 09/16/16 21:53:24 (TAI)
UTC Offset           : 36
Freq Traceable       : true
Time Traceable       : true
Time Source          : gps
```

```
================================================================================
* indicates that the corresponding row element may have been truncated.
================================================================================
Port/Peer Summary
--------------------------------------------------------------------------------
PtpPort/Peer          : 1/1
IP Address            : 10.10.10.10
Static/Dynamic        : Static
PTP Port State        : initializing
                                                    Rx          Tx
--------------------------------------------------------------------------------
Anno                                                623         0
Sync                                                82990       0
Follow-Up                                           82990       -
DelayRequest                                        82998       82998
DelayResponse                                       82998       82998
--------------------------------------------------------------------------------
================================================================================
A:7705:Dut-I#
```

Table 52: System PTP clock field descriptions

Label	Description
Local clock	
Clock Type	The local clock type
Admin State	up — the local clock is enabled and running down — the local clock is shut down and not running
Source Interface	The PTP clock source interface as configured by the source-interface command
Clock MDA	The PTP clock-mda as configured by the clock-mda command
PTP Profile	The PTP profile as configured by the profile command
Domain	The local clock domain
Clock ID	The local clock identification
Clock Class	The local clock class
Clock Accuracy	The local clock accuracy designation
Clock Variance	The local clock variance
Clock Priority1	The local clock priority1 designation
Clock Priority2	The local clock priority2 designation
Clock Local-priority	The local clock local priority designation
Steps Removed	The number of hops from the PTP grandmaster clock. This value is used by the BTCA to determine which clock should provide

Label	Description
	timing to the network when the profile is set to **g8275dot1-2014** or **g8275dot2-2016**.
Use Node Time	Indicates whether the PTP clock uses the node system time as the clock source
Dynamic Peers	Indicates whether dynamic peers are enabled
Admin Freq-source	The administrative value of the frequency source
Oper Freq-source	The operational value of the frequency source
Tx While Sync Uncert*	Indicates whether Announce messages are transmitted while the clock is in a synchronization uncertain state: true or false
Sync Certainty State	Indicates the synchronization certainty state of the local clock: certain or uncertain
Two-Step	Indicates whether the local clock uses a one-step or two-step synchronization method
Parent clock	
Parent Clock ID	The parent clock identification
Parent Port Number	The parent clock port number
GM Clock Id	The grandmaster clock ID
GM Clock Class	The grandmaster clock class
GM Clock Accuracy	The grandmaster clock accuracy designation
GM Clock Variance	The grandmaster clock variance
GM Clock Priority1	The grandmaster clock priority1 designation
GM Clock Priority2	The grandmaster clock priority2 designation
Rx Sync Certainty	Indicates the synchronization certainty state received from the parent clock: certain or uncertain
PTP Time Recovery	
Time Recovery State	The state of the time recovery algorithm: • acquiring — the algorithm is active but is not in a locked or holdover state • locked — the algorithm is generating time adjustments within the locked performance range • holdover — the algorithm has not generated time adjustments for a period of time

Label	Description
Last Changed	The date and time when the Time Recovery State field last changed
Last Offset From Master	The offsetFromMaster value, in nanoseconds, calculated from the last packet exchange with the parent clock
Last Calc	The date and time when the field was last calculated
Last Mean Path Delay	The meanPathDelay value, in nanoseconds, calculated from the last packet exchange with the parent clock
Last Adjustment	The change to the local time scale, in nanoseconds, that was last generated by the time recovery algorithm
Time information	
Timescale	The PTP timescale flag sent in the 1588 Announce message
Recovered Date/Time	The last date and time recovered by the PTP time recovery algorithm
UTC Offset	The offset between TAI and UTC, in seconds
Freq Traceable	The frequency traceable flag sent in the 1588 Announce message
Time Traceable	The time traceable flag sent in the 1588 Announce message
Time Source	The time-source parameter sent in the 1588 Announce message
Port/peer summary	
PtpPort/Peer	The PTP port and peer ID as configured in the **config>system>ptp>clock** context
IP Address	The IP address of the PTP peer
Static/Dynamic	Indicates if the peer is statically configured or dynamically requested
PTP Port State	The PTP port state: initializing, listening, uncalibrated, slave, master, or passive
Rx/Tx	The direction of the packet counts
Anno	The number of ingress or egress Announce packets
Sync	The number of ingress or egress synchronization packets
Follow-Up	The number of ingress follow-up packets
DelayRequest	The number of ingress or egress delay request packets

Label	Description
DelayResponse	The number of ingress or egress delay response packets

port

Syntax

port [*port-id* [**detail**]]

Context

show>system>ptp>clock

Description

This command displays information about configured PTP Ethernet ports. This command only applies when the *clock-id* parameter is set to **csm**.

Parameters

port-id

specifies the PTP port ID in the format *slot/mda/port*

ptp-port

Syntax

ptp-port *port-id*

Context

show>system>ptp>clock

Description

This command displays PTP port information. This command only applies when the *clock-id* parameter value is 1 to 16.

Parameters

port-id

specifies the PTP port ID

Values   1 to 50

Output

The following output is an example of PTP port information, and Table 53: System PTP port field descriptions describes the fields.

Output example

```
A:# show system ptp clock 1 ptp-port 1

===============================================================================
PTP Port
===============================================================================
Admin State          : up             Number Of Peers      : 2
Log-anno-interval    : 1              Anno-rx-timeouts     : 3
Log-sync-interval    : -6             Unicast              : True
Master-only          : false          Local-priority       : 128
PTP Port State       : slave
===============================================================================
```

Table 53: System PTP port field descriptions

Label	Description
Admin State	up –the port is administratively up down – the port is administratively down
Number Of Peers	The number of peers associated with this PTP port
Log-anno-interval	The expected interval between the reception of Announce messages
Anno-rx-timeouts	The number of Announce timeouts that need to occur before communication messages with a timeTransmitter clock are assumed lost and the timeTransmitter clock is considered not available. One timeout in this context is equal to the Announce interval in seconds, calculated using the logarithm 2^log-anno-interval-value.
Log-sync-interval	The expected interval between the reception of synchronization messages
Unicast	True — the PTP timeReceiver clock can unicast-negotiate with the PTP timeTransmitter clock False — the PTP timeReceiver clock cannot unicast-negotiate with the PTP timeTransmitter clock
Master-only	True – the local port cannot enter the timeReceiver state False – the local port can enter the timeReceiver state
Local-priority	The local priority designation of the associated clock
PTP Port State	The PTP port state: initializing, listening, uncalibrated, slave, master, or passive

peer

Syntax

peer *peer-id* [**all**] [**detail**]

Context

show>system>ptp>clock>ptp-port

Description

This command displays PTP peer information.

Parameters

peer-id

specifies the PTP peer ID

Values   1 to 50

Output

The following output is an example of detailed PTP peer information, and Table 54: System PTP port peer detailed field descriptions describes the fields.

Output example

```
*A:7705:Dut-B# show system ptp clock 2 ptp-port 1 peer 1 detail


===============================================================================
PTP Port
===============================================================================
Admin State          : up              Number Of Peers    : 1
Log-anno-interval    : 1               Anno-rx-timeouts   : 3
Log-sync-interval    : -6              Unicast            : True
Master-only          : false           Local-priority     : 128
PTP Port State       : slave
===============================================================================


===============================================================================
Peer-1
===============================================================================
IP Address           : 10.20.1.1
Current Master       : true            static/dynamic     : static
Description          : (Not Specified)
Clock Id             : 143e60fffec6f84a Port Number        : 1
GM Clock Id          : 143e60fffec6f84a GM Clock Class     : 6
GM Clock Accuracy    : 100ns           GM Clock Variance  : 20061
GM Clock Priority1   : 128             GM Clock Priority2 : 128
Step Type            : one-step        Rx Sync Certainty  : certain
APTS Asymmetry       : -752 ns
APTS Asymm Last Calc : 10/13/2023 13:14:20
Last Rx Anno Msg     : 10/13/2023 13:14:21


-------------------------------------------------------------------------------
Unicast Info
-------------------------------------------------------------------------------
Dir Type        Rate    Dur   Result        Time                  Remain
-------------------------------------------------------------------------------
```

© 2024 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
Tx  Anno       -           -       unknown        10/13/2023 11:58:58   -
    Sync       -           -       local cancel   10/13/2023 12:13:56   -
    DelayResp  -           -       local cancel   10/13/2023 12:13:56   -
Rx  Anno       1 pkt/2 s 300       granted        10/13/2023 13:11:57   154
    Sync       64 pkts/s 300       granted        10/13/2023 13:13:56   273
    DelayResp  64 pkts/s 300       granted        10/13/2023 13:13:56   273
-------------------------------------------------------------------------
===============================================================================


===============================================================================
PTP 1 Statistics
===============================================================================
                                                Input             Output
-------------------------------------------------------------------------
Signalling Packets                                 76                 76
Unicast Request Announce Packets                    0                 24
Unicast Request Announce Timeout                    0                  1
Unicast Request Announce Reject                     0
Unicast Request Sync Packets                       25                 25
Unicast Request Sync Timeout                        0                  0
Unicast Request Sync Reject                         0
Unicast Request Delay Resp Packe*                   0                 25
Unicast Request Delay Resp Timeo*                   0                  0
Unicast Request DelayResp Reject                    0
Unicast Grant Announce Packets                     24                  0
Unicast Grant Announce Rejected                     0                  0
Unicast Grant Sync Packets                         25                  0
Unicast Grant Sync Rejected                         0                  0
Unicast Grant Delay Resp Packets                   25                  0
Unicast Grant Delay Resp Rejected                                      0
Unicast Cancel Announce Packets                     0                  0
Unicast Cancel Sync Packets                         0                  1
Unicast Cancel Delay Resp Packets                   0                  1
Unicast Ack Cancel Announce Pack*                   0                  0
Unicast Ack Cancel Sync Packets                     0                  0
Unicast Ack Cancel Delay Resp Pa*                   1                  0
Anno Packets                                     1817                  0
Sync Packets                                   224947                  0
Follow-Up Packets                                   0                  0
Delay Response Packets                         224948                  0
Delay Request Packets                               0             224948
Out Of Order Sync Packets                           0
Total UDP (port 320) Pkts                      226841                 76
Total UDP (port 319) Pkts                      224947             224948


Discard Statistics
-------------------------------------------------------------------------
Alternate Master Packets                            0
Bad Domain Packets                                  0
Bad Version Packets                                 0
Duplicate Msg Packets                               0
Step RM Greater Than 255                            0
===============================================================================
* indicates that the corresponding row element may have been truncated.


===============================================================================
PTP Peer 1 Frequency Algorithm State Statistics (in seconds)
===============================================================================
  Free-run                     : 548
  Acquiring                    : 128
  Phase-Tracking               : 2840
  Hold-over                    : 0
  Locked                       : 0
```

```
===============================================================================

===============================================================================
PTP Peer 1 Frequency Algorithm Event Statistics
===============================================================================
  Excessive Freq Error Detected   : 1
  Excessive Packet Loss Detected  : 0
  Packet Loss Spotted             : 0
  Excessive Phase Shift Detected  : 0
  High PDV Detected               : 0
  Sync Packet Gaps Detected       : 0
===============================================================================
===============================================================================
PTP Peer-1 Clock Recovery
  - Internal Digital Phase Locked Loop (DPLL) Statistics
===============================================================================
                     sync    delay-req       phase       phase
                  pkt delay  pkt delay        error       error
                     stddev     stddev                   stddev
time                   (ns)       (ns)         (ns)        (ns)
-------------------------------------------------------------------------------
10/13/2023 13:13:48       0          0         2839          41
10/13/2023 13:11:48       0          0         2984          44
10/13/2023 13:09:48       0          0         3132          44
10/13/2023 13:07:48       0          0         3292          49
10/13/2023 13:05:48       0          0         3464          51
10/13/2023 13:03:48       0          0         3615          36
10/13/2023 13:01:48       0          0         3731          31
10/13/2023 12:59:48       0          0         3832          30
10/13/2023 12:57:48       0          0         3928          24
10/13/2023 12:55:48       0          0         4000          22
10/13/2023 12:53:48       0          0         4108          40
10/13/2023 12:51:48       0          0         4227          27
10/13/2023 12:49:48       0          0         4299          16
10/13/2023 12:47:48       0          0         4339           9
10/13/2023 12:45:48       0          0         4356           2
===============================================================================
```

Table 54: System PTP port peer detailed field descriptions

Label	Description
PTP Port	
Admin State	up – the port is administratively up down – the port is administratively down
Number Of Peers	The number of peers associated with this PTP port
Log-anno-interval	The expected interval between the reception of Announce messages
Anno-rx-timeouts	The number of Announce timeouts that need to occur before communication messages with a timeTransmitter clock are assumed lost and the timeTransmitter clock is considered not available. One timeout in this context is equal to the Announce interval in seconds, calculated using the logarithm 2^log-anno-interval-value.

Label	Description
Log-sync-interval	The expected interval between the reception of synchronization messages
Unicast	True — the PTP timeReceiver clock can unicast-negotiate with the PTP timeTransmitter clock
	False — the PTP timeReceiver clock cannot unicast-negotiate with the PTP timeTransmitter clock
Master-only	True – the local port cannot enter the timeReceiver state
	False – the local port can enter the timeReceiver state
Local-priority	The local priority designation of the associated clock
PTP Port State	The PTP port state: initializing, listening, uncalibrated, slave, master, or passive
Peer-1	
IP Address	The peer-1 clock IP address
Current Master	True — the peer-1 clock is the current timeTransmitter clock
	False — the peer-1 clock is not the current time Transmitter clock
Description	The peer-1 clock description
Clock ID	The peer-1 clock identification
Port Number	The peer-1 clock port number
GM Clock ID	The grandmaster clock identification
GM Clock Class	The grandmaster clock class designation
GM Clock Accuracy	The grandmaster clock accuracy designation
GM Clock Variance	The grandmaster clock scaled log variance in decimal format
GM Clock Priority1	The grandmaster clock priority1 designation
GM Clock Priority2	The grandmaster clock priority2 designation
Step Type	Indicates whether the peer-1 clock uses a one-step or two-step synchronization method
Rx Sync Certainty	Indicates the received synchronization certainty state
APTS Asymmetry	Indicates the offset value, in nanoseconds
APTS Asymm Last Calc	Indicates the last time the offset was calculated

Label	Description
Last Rx Anno Msg	The time when the last Announce message was received from the peer clock
Unicast Info	
Dir	The direction of the unicast information: either Rx or Tx
Type	The message type: Announce, Synchronization, or Delay Response
Rate	The rate of the unicast information in packets per second
Dur	The lease duration for the session
Result	The result of the last unicast request sent to the peer for the indicated message type
Time	The time the unicast information was received
Remain	The time remaining before the lease expires
PTP 1 Statistics	
	The following input/output statistics are provided for the peer-1/peer-2 clock: • Signalling Packets • Unicast Request Announce Packets • Unicast Request Announce Timeout • Unicast Request Announce Reject • Unicast Request Sync Packets • Unicast Request Sync Timeout • Unicast Request Sync Reject • Unicast Request Delay Resp Packets • Unicast Request Delay Resp Timeout • Unicast Request Delay Resp Reject • Unicast Grant Announce Packets • Unicast Grant Announce Rejected • Unicast Grant Sync Packets • Unicast Grant Sync Rejected • Unicast Grant Delay Resp Packets • Unicast Grant Delay Resp Rejected • Unicast Cancel Announce Packets • Unicast Cancel Sync Packets

Label	Description
	• Unicast Cancel Delay Resp Packets • Unicast Ack Cancel Announce Packets • Unicast Ack Cancel Sync Packets • Unicast Ack Cancel Delay Resp Packets • Anno Packets • Sync Packets • Follow-Up Packets • Delay Response Packets • Delay Request Packets • Out Of Order Sync Packets • Total UDP (port 320) Pkts • Total UDP (port 319) Pkts
	The following discard statistics are provided for the peer-1/peer-2 clock: • Alternate Master Packets • Bad Domain Packets • Bad Version Packets • Duplicate Msg Packets • Step RM Greater Than 255
	The following algorithm state statistics (in seconds) are provided for the peer-1/peer-2 clock: • Free-run • Acquiring • Phase-Tracking • Hold-over • Locked
	The following algorithm event statistics are provided for the peer-1/peer-2 clock: • Excessive Freq Error Detected • Excessive Packet Loss Detected • Packet Loss Spotted • Excessive Phase Shift Detected • High PDV Detected • Sync Packet Gaps Detected

Label	Description
	The following statistics are shown for the peer clock. These statistics are refreshed every 2 min; the display shows the time of the last update: • sync pkt delay stddev (ns) • delay-req pkt delay stddev (ns) • phase error (ns) • phase error stddev (ns)

rollback

Syntax

rollback [**rescue**]

Context

show>system

Description

This command displays CLI configuration rollback checkpoint file information.

Parameters

rescue

displays CLI configuration rollback rescue file information

Output

The following outputs are examples of rollback information and rollback rescue information, and Table 55: System rollback field descriptions describes the fields.

Output example

```
*A:7705:Dut-C# show system rollback
===========================================================================
Rollback Information
===========================================================================
Rollback Location          : ftp://*:*@xxx.xxx.xxx.xx//device_logs/Dut-C-Rollback
Max Local  Rollback Files  : 10
Max Remote Rollback Files  : 10
Save
  Last Rollback Save Result  : Successful
  Last Save Completion Time  : 2017/01/25 22:42:47 UTC
Revert
  In Progress              : No
  Last Revert Initiated User : N/A
  Last Revert Checkpoint File: N/A
  Last Revert Result       : None
  Last Revert Initiated Time : N/A
  Last Revert Completion Time: N/A
Delete
```

```
    Last Rollback Delete Result: None
===============================================================================
Rollback Files
===============================================================================
Idx    Suffix    Creation Time           Release        User
          Comment
-------------------------------------------------------------------------------
latest .rb       2017/01/25 22:42:45 UTC  B-8.0.B1-R4    admin
          L3_SPOKE_SETUP
1      .rb.1     2017/01/25 22:33:58 UTC  B-8.0.B1-R4    admin
2      .rb.2     2017/01/25 22:25:46 UTC  B-8.0.B1-R4    admin
          L3_SPOKE_SETUP
3      .rb.3     2017/01/25 19:49:30 UTC  B-8.0.B1-R4    admin
4      .rb.4     2017/01/25 19:44:42 UTC  B-8.0.B1-R4    admin
          L3_SPOKE_SETUP
5      .rb.5     2017/01/25 19:14:51 UTC  B-8.0.B1-R4    admin
          Firewall with NGE rollback
6      .rb.6     2017/01/25 19:04:16 UTC  B-8.0.B1-R4    admin
          initial
-------------------------------------------------------------------------------
No. of Rollback Files: 7
===============================================================================
*A:7705:Dut-C#
```

```
*A:Sar8 Dut-A# show system rollback rescue
===============================================================================
Rollback Rescue Information
===============================================================================
Rollback Rescue Location     : cf3:/rescue
  Rescue file saved          : Yes
Save
  Last Save Result           : Successful
  Last Save Completion Time  : 2017/02/24 17:54:57 UTC
Revert
  In Progress                : No
  Last Revert Initiated User : admin
  Last Revert Result         : Successful
  Last Revert Initiated Time : 2017/02/24 17:55:09 UTC
  Last Revert Completion Time: 2017/02/24 17:55:09 UTC
Delete
  Last Delete Result         : None
*A:Sar8 Dut-A#
```

Rollback rescue output example

```
*A:Sar8 Dut-A# show system rollback rescue
===============================================================================
Rollback Rescue Information
===============================================================================
Rollback Rescue Location     : cf3:/rescue
  Rescue file saved          : Yes
Save
  Last Save Result           : Successful
  Last Save Completion Time  : 2017/02/24 17:54:57 UTC
Revert
  In Progress                : No
  Last Revert Initiated User : admin
  Last Revert Result         : Successful
  Last Revert Initiated Time : 2017/02/24 17:55:09 UTC
  Last Revert Completion Time: 2017/02/24 17:55:09 UTC
Delete
  Last Delete Result         : None
```

```
*A:Sar8 Dut-A#
```

Table 55: System rollback field descriptions

Label	Description
Rollback Information	
Rollback Location	The location where rollback checkpoint files will be saved
Max Local Rollback Files	The maximum number of rollback checkpoint files that will be saved to a local server
Max Remote Rollback Files	The maximum number of rollback checkpoint files that will be saved to a remote server
Save	
Last Rollback Save Result	The status of the last rollback checkpoint save
Last Save Completion Time	The date and time the last rollback checkpoint file save operation was completed
Revert	
In Progress	Indicates if a system rollback reversion is in progress
Last Revert Initiated User	The username of the person who initiated the last system rollback reversion
Last Revert Checkpoint File	The location of the last rollback checkpoint file
Last Revert Result	The result of the last system rollback reversion
Last Revert Initiated Time	The date and time when the last rollback was initiated
Last Revert Completion Time	The date and time when the last rollback was completed
Delete	
Last Rollback Delete Result	The status of the last rollback checkpoint file deletion
Rollback Files	
Idx	The rollback checkpoint file ID
Suffix	The rollback checkpoint file suffix
Comment	User comments about the rollback checkpoint file

Label	Description
Creation Time	The date and time when the file was created
Release	The software load that the checkpoint file was created in
User	The user who created the file
Rollback Rescue Information	
Rollback Rescue Location	The location where rollback rescue files will be saved
Rescue file saved	The maximum number of rollback rescue files that will be saved to a local server
Save	
Last Save Result	The status of the last rollback checkpoint save
Last Save Completion Time	The date and time the last rollback rescue file save operation was completed
Revert	
In Progress	Indicates if a system rollback reversion is in progress
Last Revert Initiated User	The username of the person who initiated the last system rollback reversion
Last Revert Result	The result of the last system rollback reversion
Last Revert Initiated Time	The date and time when the last rollback was initiated
Last Revert Completion Time	The date and time when the last rollback was completed
Delete	
Last Delete Result	The status of the last rollback rescue file deletion

script-control

Syntax

script-control

Context

show>system

Description

This command enables the context to display script information.

script

Syntax

script [*script-name*] [**owner** *script-owner*]

Context

show>system>script-control

Description

This command displays script parameters.

Parameters

script-name

displays information for the specified script name

script-owner

displays information for the specified script owner associated with the script name

Output

The following output is an example of script information, and Table 56: Script field descriptions describes the fields.

Output example

```
A:ALU-1# show system script-control script
===============================================================================
Script Information
===============================================================================
Script                     : test
Owner name                 : TiMOS CLI
Description                : asd
Administrative status      : enabled
Operational status         : enabled
Script source location     : ftp://*****:******@192.168.100.1/home/testlab_bgp
                             /test1.cfg
Last script error          : none
Last change                : 2017/01/07 17:10:03
===============================================================================
A:ALU-1#
```

Table 56: Script field descriptions

Label	Description
Script	The name of the script
Owner name	The name of the script owner

Label	Description
Description	The description of the script
Administrative status	Enabled — administrative status is enabled Disabled — administrative status is disabled
Operational status	Enabled — operational status is enabled Disabled — operational status is disabled
Script source location	The location of the scheduled script
Last script error	The system time of the last error
Last change	The system time of the last change to the script configuration

script-policy

Syntax

script-policy *policy-name* [**owner** *policy-owner*]

script-policy run-history [*run-state*]

Context

show>system>script-control

Description

This command displays script policy information.

Parameters

policy-name

displays information for the specified script policy name

policy-owner

displays information for the specified script policy owner associated with the script policy name

run-state

displays information for script policies in the specified state

Values   executing, initializing, terminated

Output

The following output is an example of script policy information, and Table 57: Script policy field descriptions describes the fields.

Output example

```
A:ALU-1# show system script-control script-policy "test_policy"
===============================================================================
Script-policy Information
===============================================================================
Script-policy             : test_policy
Script-policy Owner       : TiMOS CLI
Administrative status     : enabled
Operational status        : enabled
Script                    : test_script
Script owner              : TiMOS CLI
Script source location    : ftp://*****:******@192.168.100.1/home/testlab_bgp
                            /test1.cfg
Script results location   : ftp://*****:******@192.168.15.1/home/testlab_bgp
                            /cron/res
Max running allowed       : 1
Max completed run histories  : 4
Max lifetime allowed      : 0d 01:00:00 (3600 seconds)
Completed run histories   : 1
Executing run histories   : 0
Initializing run histories  : 0
Max time run history saved : 0d 02:00:00 (7200 seconds)
Script start error        : N/A
Last change               : 2018/07/03 18:02:36
Max row expire time       : never
Last application          : event-script
Last auth. user account   : not-specified
===============================================================================
Script Run History Status Information
-------------------------------------------------------------------------------
No script run history entries
===============================================================================
A:ALU-1#
```

```
A:ALU-1# show system script-control script-policy run-history terminated
===============================================================================
Script-policy Run History
===============================================================================
Script policy "test"
Owner "TiMOS CLI"
-------------------------------------------------------------------------------
Script Run #17
-------------------------------------------------------------------------------
Start time : 2017/11/06 20:30:09    End time : 2017/11/06 20:35:24
Elapsed time : 0d 00:05:15          Lifetime : 0d 00:00:00
State : terminated                  Run exit code : noError
Result time : 2017/11/06 20:35:24   Keep history : 0d 00:49:57
Error time : never
Results file : ftp://*:*@192.168.15.18/home/testlab_bgp/cron/_20171106-203008.
out
Run exit : Success
-------------------------------------------------------------------------------
Script Run #18
-------------------------------------------------------------------------------
Start time : 2017/11/06 20:35:24    End time : 2017/11/06 20:40:40
Elapsed time : 0d 00:05:16          Lifetime : 0d 00:00:00
State : terminated                  Run exit code : noError
Result time : 2017/11/06 20:40:40   Keep history : 0d 00:55:13
Error time : never
Results file : ftp://*:*@192.168.15.18/home/testlab_bgp/cron/_20171106-203523.
out
Run exit : Success
```

```
--------------------------------------------------------------------------------
A:ALU-1#


A:ALU-1# show system script-control script-policy run-history executing
===============================================================================
Script-policy Run History
===============================================================================
Script policy "test"
Owner "TiMOS CLI"
-------------------------------------------------------------------------------
Script Run #20
-------------------------------------------------------------------------------
Start time : 2017/11/06 20:46:00     End time : never
Elapsed time : 0d 00:00:56           Lifetime : 0d 00:59:04
State : executing                    Run exit code : noError
Result time : never                  Keep history : 0d 01:00:00
Error time : never
Results file : ftp://*:*@192.168.15.18/home/testlab_bgp/cron/_20171106-204559.
out
===============================================================================
A:ALU-1# show system script-control script-policy run-history initializing
===============================================================================
Script-policy Run History
===============================================================================
Script policy "test"
Owner "TiMOS CLI"
-------------------------------------------------------------------------------
Script Run #21
-------------------------------------------------------------------------------
Start time : never                   End time : never
Elapsed time : 0d 00:00:00           Lifetime : 0d 01:00:00
State : initializing                 Run exit code : noError
Result time : never                  Keep history : 0d 01:00:00
Error time : never
Results file : none
-------------------------------------------------------------------------------
Script Run #22
-------------------------------------------------------------------------------
Start time : never                   End time : never
Elapsed time : 0d 00:00:00           Lifetime : 0d 01:00:00
State : initializing                 Run exit code : noError
Result time : never                  Keep history : 0d 01:00:00
Error time : never
Results file : none
-------------------------------------------------------------------------------
Script Run #23
-------------------------------------------------------------------------------
Start time : never                   End time : never
Elapsed time : 0d 00:00:00           Lifetime : 0d 01:00:00
State : initializing                 Run exit code : noError
Result time : never                  Keep history : 0d 01:00:00
Error time : never
Results file : none
===============================================================================
A:ALU-1#
```

Table 57: Script policy field descriptions

Label	Description
Script-policy	The name of the script policy

Label	Description
Script-policy Owner	The name of the script policy owner
Administrative status	Enabled — administrative status is enabled Disabled — administrative status is disabled
Operational status	Enabled — operational status is enabled Disabled — operational status is disabled
Script	The name of the script
Script owner	The name of the script owner
Script source location	The location of the scheduled script
Script results location	The location where the script results are sent
Max running allowed	The maximum number of allowed script runs
Max completed run histories	The maximum number of run history status entries that can be kept
Max lifetime allowed	The maximum length of time that the script may run
Completed run histories	The number of completed script runs
Executing run histories	The number of script runs in the process of executing
Initializing run histories	The number of scripts queued to run but not executed
Max time run history saved	The maximum length of time to keep the run history status entry
Script start error	Indicates if any errors occurred when starting the script
Last change	The system time of the last change made to the script policy configuration
Max row expire time	The length of time that an entry (row) in the smLaunchTable (in the Script MIB) is kept and available to launch an associated script before it is deleted. Entries are deleted if there are no associated scripts in the run history. On the 7705 SAR, this timer cannot be set; therefore, the status is always Never (the row is never deleted).
Last application	The last application that triggered the script run

Label	Description
Last auth. user account	The last user account that the script was executed under in order for authorization to be performed
Script Run History Status Information	
Script Run #	Indicates the number of times that the script has run
Start time	The time that the script run started
End time	The time that the script run ended
Elapsed time	The length of time between start and end of the script run
Lifetime	The maximum length of time that the script may run
State	The state of the script: executing, initializing, or terminated
Run exit code	The code generated at the end of the script run (for example, no Error)
Result time	The time that the script results were generated
Keep history	The length of time to keep the script run history status entry
Error time	The time during the script run at which an error occurred
Results file	The location where the script results are stored
Run exit	Indicates whether the run completed successfully

sntp

Syntax

   sntp

Context

   show>system

Description

   This command displays SNTP protocol configuration and state.

Output

   The following output is an example of SNTP information, and Table 58: System SNTP field descriptions describes the fields.

   Output example

```
A:ALU-1# show system sntp
```

```
=================================================================
SNTP Status
=================================================================
Admin Status : up          Oper Status : up          Mode : unicast
=================================================================


=================================================================
SNTP
Servers
=================================================================
SNTP Server          Version          Preference      Interval
-----------------------------------------------------------------
10.10.20.253         3               Preferred        64
=================================================================
A:ALU-1#
```

Table 58: System SNTP field descriptions

Label	Description
Admin Status	up — the SNTP server is administratively up
	down — the SNTP server is administratively down
Oper Status	up — the SNTP server is operationally up
	down — the SNTP server is operationally down
Mode	broadcast — the SNTP server has broadcast client mode enabled
	unicast — the SNTP server has unicast client mode enabled
SNTP Server	The SNTP server address for SNTP unicast client mode
Version	The SNTP version number, expressed as an integer
Preference	Normal — when more than one time server is configured, one server can be configured to have preference over another
	Preferred — indicates that this server has preference over another
Interval	The frequency, in seconds, that the server is queried

thresholds

Syntax

thresholds

Context

show>system

Description

This command display system monitoring thresholds.

Output

The following output is an example of system monitoring thresholds information, and Table 59: System threshold field descriptions describes the fields.

Output example

```
A:ALU-48# show system thresholds
===============================================================
Threshold Alarms
===============================================================
Variable: tmnxCpmFlashUsed.1.11.1
Alarm Id       : 1        Last Value : 835
Rising Event Id  : 1        Threshold  : 5000
Falling Event Id : 2        Threshold  : 2500
Sample Interval  : 2748341* SampleType : absolute
Startup Alarm    : either   Owner      : TiMOS CLI

Variable: tmnxCpmFlashUsed.1.11.1
Alarm Id       : 2        Last Value : 835
Rising Event Id  : 3        Threshold  : 10000
Falling Event Id : 4        Threshold  : 5000
Sample Interval  : 27483    SampleType : absolute
Startup Alarm    : rising   Owner      : TiMOS CLI

Variable: sgiMemoryUsed.0
Alarm Id       : 3        Last Value : 42841056
Rising Event Id  : 5        Threshold  : 4000
Falling Event Id : 6        Threshold  : 2000
Sample Interval  : 2147836  SampleType : absolute
Startup Alarm    : either   Owner      : TiMOS CLI


===============================================================
* indicates that the corresponding row element may have been truncated.
===============================================================
Threshold Events
===============================================================
Description: TiMOS CLI - cflash capacity alarm rising event
Event Id       : 1        Last Sent  : 10/31/2006 08:47:59
Action Type    : both     Owner      : TiMOS CLI

Description: TiMOS CLI - cflash capacity alarm falling event
Event Id       : 2        Last Sent  : 10/31/2006 08:48:00
Action Type    : both     Owner      : TiMOS CLI

Description: TiMOS CLI - cflash capacity warning rising event
Event Id       : 3        Last Sent  : 10/31/2006 08:47:59
Action Type    : both     Owner      : TiMOS CLI

Description: TiMOS CLI - cflash capacity warning falling event
Event Id       : 4        Last Sent  : 10/31/2006 08:47:59
Action Type    : both     Owner      : TiMOS CLI

Description: TiMOS CLI - memory usage alarm rising event
Event Id       : 5        Last Sent  : 10/31/2006 08:48:00
Action Type    : both     Owner      : TiMOS CLI

Description: TiMOS CLI - memory usage alarm falling event
Event Id       : 6        Last Sent  : 10/31/2006 08:47:59
Action Type    : both     Owner      : TiMOS CLI
```

```
============================================================

============================================================
Threshold Events Log
============================================================
Description       : TiMOS CLI - cflash capacity alarm falling eve
                    nt : value=835, <=2500 : alarm-index 1, event
                    -index 2 alarm-variable OID tmnxCpmFlashUsed.
                    1.11.1
Event Id          : 2        Time Sent  : 10/31/2006 08:48:00

Description       : TiMOS CLI - memory usage alarm rising event :
                     value=42841056, >=4000 : alarm-index 3, even
                    t-index 5 alarm-variable OID sgiMemoryUsed.0
Event Id          : 5        Time Sent  : 10/31/2006 08:48:00

============================================================
A:ALU-48#
```

Table 59: System threshold field descriptions

Label	Description
Variable	The variable OID
Alarm Id	The numerical identifier for the alarm
Last Value	The last threshold value
Rising Event Id	The identifier of the RMON rising event
Threshold	The identifier of the RMON rising threshold
Falling Event Id	The identifier of the RMON falling event
Threshold	The identifier of the RMON falling threshold
Sample Interval	The polling interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds
Startup Alarm	The alarm that may be sent when this alarm is first created
Owner	The owner of this alarm
Description	The event cause
Event Id	The identifier of the threshold event
Last Sent	The date and time the alarm was sent
Action Type	log — an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

Label	Description
	trap — a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.
	both — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated
	none — no action is taken
Owner	The owner of the event

time

Syntax

time [**detail**]

Context

show>system

Description

This command displays the system time and zone configuration parameters.

Output

The following outputs are examples of time information:

- 7705 SAR-8 Shelf V2, 7705 SAR-18 (Output example, Table 60: System Time Field Descriptions (7705 SAR-8 Shelf V2, 7705 SAR-18))
- 7705 SAR chassis where GNSS and PTP are used as sources of system time (Detailed output example, Table 61: System time field descriptions (GNSS and PTP time source))

Output example

```
A:ALU-1# show system time
===============================================================================
Date & Time
===============================================================================
Current Date & Time : 2014/08/13 20:47:23    DST Active           : no
Current Zone        : UTC                     Offset from UTC      : 0:00
-------------------------------------------------------------------------------
Non-DST Zone        : UTC                     Offset from UTC      : 0:00
Zone type           : standard
-------------------------------------------------------------------------------
DST Zone            : PDT                      Offset from Non-DST  : 0:60
Starts              : first sunday in april 02:00
Ends                : last sunday in october 02:00
===============================================================================
```

Table 60: System Time Field Descriptions (7705 SAR-8 Shelf V2, 7705 SAR-18)

Label	Description
Current Date & Time	The system date and time using the current time zone
DST Active	Yes — Daylight Savings Time is currently in effect
	No — Daylight Savings Time is not currently in effect
Current Zone	The zone name for the current zone
Non-DST Zone	The zone name for the non-DST zone
DST Zone	The zone name for the DST zone
Zone type	Non-standard — the zone is user-defined
	Standard — the zone is system-defined
Offset from UTC	The number of hours and minutes added to universal time for the current zone and non-DST zone, including the DST offset for a DST zone
Offset from Non-DST	The number of hours (always 0) and minutes (0 to 60) added to the time at the beginning of Daylight Saving Time and subtracted at the end of Daylight Saving Time
Starts	The date and time Daylight Saving Time begins
Ends	The date and time Daylight Saving Time ends

Detailed output example

```
A:ALU-1# show system time detail
===============================================================================
Date & Time
===============================================================================
Current Date & Time : 2014/08/13 20:47:23    DST Active           : no
Current Zone        : UTC                    Offset from UTC      : 0:00
-------------------------------------------------------------------------------
Non-DST Zone        : UTC                    Offset from UTC      : 0:00
Zone type           : standard
-------------------------------------------------------------------------------
DST Zone            : PDT                    Offset from Non-DST  : 0:60
Starts              : first sunday in april 02:00
Ends                : last sunday in october 02:00
===============================================================================
Time References
===============================================================================
Selected Ref    : gps 1/3/1        Selection Time  : 08/13/2014 20:23:19
-------------------------------------------------------------------------------
time-ref-prior*: 1                 Selected         : true
Ref Type        : gps              Qualified        : true
Ref Id          : 1/3/1           Leap Sec Sched    : notScheduled
Delta Sec       : 0               Leap Sec Upd Time: n/a
Delta Ns        : 0
```

```
-------------------------------------------------------------------------
time-ref-prior*: 2                      Selected        : false
Ref Type        : ptp                   Qualified       : false
Ref Id          : clock 1               Leap Sec Sched  : notScheduled
Delta Sec       : 0                     Leap Sec Upd Time: n/a
Delta Ns        : 0
-------------------------------------------------------------------------
=========================================================================
* indicates that the corresponding row element may have been truncated
=========================================================================
Time Of Day - 1 Pulse Per Second Port
=========================================================================
Output          : no shutdown           Message Type   : none
-------------------------------------------------------------------------
Format          : IRIG-B
Modulation      : 0 = Digital            Modulation      : 1 = Amplitude Modulated
Freq/Resolution: 0 = No Carrier          Freq/Resolution: 2 = 1 kHz/1 ms
Coded Expressi*: unknown                 Coded Expressi*:unknown
=========================================================================
* indicates that the corresponding row element may have been truncated
```

Table 61: System time field descriptions (GNSS and PTP time source)

Label	Description
Current Date & Time	The system date and time using the current time zone
DST Active	Yes — Daylight Savings Time is currently in effect
	No — Daylight Savings Time is not currently in effect
Current Zone	The zone name for the current zone
Non-DST Zone	The zone name for the non-DST zone
DST Zone	The zone name for the DST zone
Zone type	Non-standard — the zone is user-defined
	Standard — the zone is system-defined
Offset from UTC	The number of hours and minutes added to universal time for the current zone and non-DST zone, including the DST offset for a DST zone
Offset from Non-DST	The number of hours (always 0) and minutes (0 to 60) added to the time at the beginning of Daylight Saving Time and subtracted at the end of Daylight Saving Time
Starts	The date and time Daylight Saving Time begins
Ends	The date and time Daylight Saving Time ends
Time References	
Selected Ref	The type and identifier of the current system time reference source

Label	Description
Selection Time	The date and time when the current system time reference source was selected to update the system time
time-ref-priority	The priority value of the time reference. A lower numeric value represents a higher priority. The time-ref-priority value must be present when the time reference is created.
Ref Type	The type of system time reference: GNSS or PTP
Ref Id	The unique identifier for the type of system time reference
Delta Sec	The time difference between this reference and the currently selected time reference in seconds. If this time reference is not qualified, the value will be 0.
Delta Ns	The time difference between this reference and the currently selected time reference in nanoseconds. If this time reference is not qualified, the value will be 0.
Selected	true — the source is being used to update system time
	false — the source is not being used to update system time
Qualified	true — the time reference is providing time updates
	false — the time reference is not providing time updates
Leap Sec Sched	Indicates whether there is a scheduled leap second
Leap Sec Upd Time	The UTC time when the scheduled leap second adjustment will occur. If a leap second is not scheduled, the value will be 0.
Time of Day - 1 Pulse Per Second Port	
Output	The state of the output: shutdown or no shutdown
Message Type	The type of message: ct, cm, or none
Format	The format of the time of day output
Modulation	The modulation type of the time of day output
Freq/Resolution	The frequency (in kHz) and resolution (in milliseconds) of the time of day output
Coded Expression	The coded expression of the time of day output

time

Syntax

time

Context

show

Description

This command displays the current day, date, time and time zone.

The time is displayed either in the local time zone or in UTC depending on the setting of the root level **time-display** command for the console session.

Output

The following output is an example of time information.

Output example

```
A:ALU-1# show time
Tue Mar 25 12:17:15 GMT 2008
A:ALU-1#
---------------------------------
```

redundancy

Syntax

redundancy

Context

show

Description

This command enables the context to show redundancy information.

multi-chassis

Syntax

multi-chassis

Context

show>redundancy

Description

This command enables the context to show multi-chassis redundancy information.

all

Syntax

all

Context

show>redundancy>multi-chassis

Description

This command displays summary multi-chassis redundancy status information.

Output

The following output is an example of general chassis information, and Table 62: Multi-chassis field descriptions describes the fields.

Output example

```
A:7705:Dut-D>config>redundancy>multi-chassis# show redundancy multi-chassis all
===============================================================================
Multi-Chassis Peers
===============================================================================
Peer IP        Src IP          Auth       Peer Admin   MC-Ring Oper MC-EP Adm
  MCS Admin      MCS Oper        MCS State  MC-LAG Adm   MC-LAG Oper
-------------------------------------------------------------------------------
10.10.10.3     10.10.10.4      None       Enabled      unknown      --
  --             --              --         Enabled      Enabled
===============================================================================
```

Table 62: Multi-chassis field descriptions

Label	Description
Peer IP	Displays the multi-chassis redundancy peer IP address
Src IP	Displays the source IP address used to communicate with the multi-chassis peer
Auth	If configured, displays the authentication key used between this node and the multi-chassis peer
Peer Admin	Displays whether the multi-chassis peer is enabled or disabled
MC-Ring Oper	Displays whether multi-chassis ring functionality is enabled or disabled. Not Applicable.

Label	Description
MC-EP Adm	Displays whether the multi-chassis endpoint is enabled or disabled (not applicable)
MCS Admin	Displays the multi-chassis synchronization is enabled or disabled (not applicable)
MCS Oper	Displays whether multi-chassis synchronization functionality is enabled or disabled (not applicable)
MCS State	Displays the multi-chassis synchronization state (not applicable)
MC-LAG Adm	Displays whether MC-LAG is enabled or disabled
MC-LAG Oper	Displays whether MC-LAG functionality is enabled or disabled

mc-firewall

Syntax

mc-firewall peer [*ip-address*]

mc-firewall peer [*ip-address*] **statistics**

mc-firewall statistics

Context

show>redundancy>multi-chassis

Description

This command displays multi-chassis firewall information.

Parameters

ip-address

shows information for the peer with the specified IP address

statistics

shows either multi-chassis firewall statistics for the specified peer or multi-chassis firewall global statistics when no peer is specified

Output

The following output is an example of multi-chassis firewall information, and Table 63: Multi-chassis firewall field descriptions describes the fields.

Output example

```
*A:Sar8 Dut-A>show>redundancy>multi-chassis# mc-firewall peer
===============================================================================
Multi-Chassis MC-Firewall
===============================================================================
```

```
Peer Addr        : 10.0.0.1          Peer Name        :
Admin State      : down              Oper State       : down
Source Addr      : 0.0.0.0           Election Role    : -
Policy Sync      : -                 Session DB Sync  : -
System Id        : d6:64:ff:00:00:00 Sys Priority     : 0
Keep Alive Intvl : 10                Hold on Nbr Fail : 3
Boot Timer       : 300
Encryption       : disabled          Active Out Spi   : -
Auth Algorithm   : -                 Encr Algorithm   : -
Sec Assoc Spi    : -                 Sec Assoc Spi    : -
Last update      : 06/27/2019 18:53:35 Last State chg  : 06/27/2019 18:53:35
-------------------------------------------------------------------------------
===============================================================================
Number of Entries 1
===============================================================================

*A:Sar8 Dut-A>show>redundancy>multi-chassis# mc-firewall peer 50.0.0.1
===============================================================================
Multi-Chassis MC-Firewall
===============================================================================
Peer Addr        : 50.0.0.1          Peer Name        :
Admin State      : up                Oper State       : up
Source Addr      : 0.0.0.0           Election Role    : Master
Policy Sync      : Yes               Session DB Sync  : Yes
System Id        : 84:db:fc:cb:ce:8d Sys Priority     : 1
Keep Alive Intvl : 10                Hold on Nbr Fail : 3
Boot Timer       : 300
Encryption       : enabled           Active Out Spi   : 1
Auth Algorithm   : sha256            Encr Algorithm   : aes128
Sec Assoc Spi    : 1                 Sec Assoc Spi    : -
Last update      : 08/19/2019 19:56:58 Last State chg  : 08/19/2019 19:43:10
===============================================================================
*A:Sar8 Dut-A>show>redundancy>multi-chassis#


*A:Sar8 Dut-A>show>redundancy>multi-chassis# mc-firewall peer 10.0.0.1 statistics
===============================================================================
Multi-Chassis MC-Firewall Statistics
===============================================================================
Peer Addr                      : 10.0.0.1
-------------------------------------------------------------------------------
Packets Rx                     : 0
Packets Rx Keepalive           : 0
Packets Rx Peer Config         : 0
Packets Rx Peer Data           : 0
Packets Dropped Rx Peer Data   : 0
Packets Dropped State Disabled : 0
Packets Dropped Packets Too Short : 0
Packets Dropped Tlv Invalid Size  : 0
Packets Dropped Out of Seq     : 0
Packets Dropped Unknown Tlv    : 0
Packets Dropped MD5            : 0
Packets Tx                     : 0
Packets Tx Keepalive           : 0
Packets Tx Peer Config         : 0
Packets Tx Peer Data           : 0
Packets Tx Failed              : 0
Packets Dropped No Peer        : 0
===============================================================================
*A:Sar8 Dut-A>show>redundancy>multi-chassis#


*A:Sar8 Dut-A>show>redundancy>multi-chassis# mc-firewall statistics
===============================================================================
```

```
Multi-Chassis Firewall Global Statistics
===============================================================================
Packets Rx                                   : 0
Packets Rx Keepalive                         : 0
Packets Rx Peer Config                       : 0
Packets Rx Peer Data                         : 0
Packets Dropped Keep-Alive Task              : 0
Packets Dropped Peer Data                    : 0
Packets Dropped Too Short                    : 0
Packets Dropped Verify Failed                : 0
Packets Dropped Tlv Invalid Size             : 0
Packets Dropped Out Of Seq                   : 0
Packets Dropped Unknown Tlv                  : 0
Packets Dropped MD5                          : 0
Packets Dropped Unknown Peer                 : 0
Packets Dropped MC Firewall No Peer          : 0
Packets Tx                                   : 0
Packets Tx Keepalive                         : 0
Packets Tx Peer Config                       : 0
Packets Tx Peer Data                         : 0
Packets Tx Failed                            : 0
===============================================================================
*A:Sar8 Dut-A>show>redundancy>multi-chassis#
```

Table 63: Multi-chassis firewall field descriptions

Label	Description
Multi-Chassis MC-Firewall	
Peer Addr	The IP address of the multi-chassis firewall peer
Peer Name	The name of the multi-chassis firewall peer
Admin State	The administrative state of the multi-chassis firewall on this system
Oper State	The operational state of the multi-chassis firewall on this system
Source Addr	The source address of the multi-chassis firewall on this system
Election Role	The elected role of the multi-chassis firewall on this system, either master or slave
Policy Sync	Indicates whether security policy synchronization has occurred on the multi-chassis firewall on this system
Session DB Sync	Indicates whether security session database synchronization has occurred on the multi-chassis firewall on this system
System Id	The system ID of the multi-chassis firewall on this system
Sys Priority	The system priority of the multi-chassis firewall on this system
Keep Alive Intvl	The time interval between keepalive messages exchanged between peers

Label	Description
Hold on Nbr Fail	Indicates how many keepalive intervals a router will wait for packets from its neighbor before declaring communication failure
Boot Timer	The configured boot timer interval
Encryption	Indicates whether encryption is enabled on the multi-chassis link (MCL)
Active Out spi	The index number of the active outbound security association
Auth Algorithm	The configured authentication algorithm, either sha256 or sha512
Encr Algorithm	The configured encryption algorithm, either aes128 or aes256
Sec Assoc Spi	The security parameter index for the security association
Last update	The date and time of the last update for the multi-chassis firewall on this system
Last State chg	The date and time of the last state change for the multi-chassis firewall on this system
Multi-Chassis MC-Firewall Statistics	
Peer Addr	The IP address of the multi-chassis firewall peer
Packets Rx	The number of packets received from the peer
Packets Rx Keepalive	The number of multi-chassis firewall keepalive packets received from the peer
Packets Rx Peer Config	The number of multi-chassis firewall configuration packets received from the peer
Packets Rx Peer Data	The number of data packets received from the peer
Packets Dropped Rx Peer Data	The number of data packets received from the peer that were dropped on this system
Packets Dropped State Disabled	The number of packets that were dropped because this system was administratively disabled
Packets Dropped Packets Too Short	The number of packets dropped because the packet was too short
Packets Dropped Tlv Invalid Size	The number of packets that were dropped because the packet was an invalid size
Packets Dropped Out Of Seq	The number of packets that were dropped because the packets were out of sequence

Label	Description
Packets Dropped Unknown Tlv	The number of packets that were dropped because the packet contained an unknown TLV
Packets Dropped MD5	The number of packets that were dropped because the packet failed MD5 authentication
Packets Tx	The number of packets transmitted from this system to the peer
Packets Tx Keepalive	The number of keepalive packets transmitted from this system to the peer
Packets Tx Peer Config	The number of configured packets transmitted from this system to the peer
Packets Tx Peer Data	The number of data packets transmitted from this system to the peer
Packets Tx Failed	The number of packets that failed to be transmitted from this system to the peer
Packets Dropped No Peer	The number of packets dropped because there is no peer
Multi-Chassis Firewall Global Statistics	
Packets Rx	The number of packets received by the system
Packets Rx Keepalive	The number of keepalive packets received by the system
Packets Rx Peer Config	The number of multi-chassis firewall configuration packets received from the peer
Packets Rx Peer Data	The number of data packets received from the peer
Packets Dropped Keep-Alive Task	The number of packets dropped by the multi-chassis firewall receiving task
Packets Dropped Peer Data	The number of data packets dropped by this system
Packets Dropped Too Short	The number of packets dropped because they were too short
Packets Dropped Verify Failed	The number of packets dropped because they could not be verified
Packets Dropped Tlv Invalid Size	The number of packets that were dropped because the packet was an invalid size
Packets Dropped Out of Seq	The number of packets that were dropped because the packets were out of sequence

Label	Description
Packets Dropped Unknown Tlv	The number of packets that were dropped because the packet contained an unknown TLV
Packets Dropped MD5	The number of packets that were dropped because the packet failed MD5 authentication
Packets Dropped Unknown Peer	The number of packets dropped because the multi-chassis firewall peer is unknown
Packets Dropped MC Firewall No Peer	The number of packets dropped because there is no multi-chassis firewall peer
Packets Tx	The number of packets transmitted
Packets Tx Keepalive	The number of keepalive packets transmitted
Packets Tx Peer Config	The number of configured packets transmitted from this system to the peer
Packets Tx Peer Data	The number of data packets transmitted from this system to the peer
Packets Tx Failed	The number of packets that failed to be transmitted

mc-lag

Syntax

mc-lag peer *ip-address* [**lag** *lag-id*]

mc-lag [**peer** *ip-address* [**lag** *lag-id*]] **statistics**

Context

show>redundancy>multi-chassis

Description

This command displays multi-chassis LAG information.

Parameters

ip-address

shows information for the peer with the specified IP address

lag-id

shows information for the specified LAG identifier

Values   1 to 32

statistics

shows statistics for the specified LAG identifier

Output

The following output is an example of MC-LAG information, and Table 64: MC-LAG field descriptions describes the fields.

Output example

```
A:ALU-1>show>redundancy>multi-chassis# mc-lag peer 10.10.10.4
===============================================================================
Multi-Chassis MC-Lag Peer 10.10.10.4
===============================================================================
Last State chg  : 01/28/2013 12:52:21
Admin State     : Up                   Oper State         : Up
KeepAlive       : 10 deci-seconds      Hold On Ngbr Failure : 3
-------------------------------------------------------------------------------
Lag Id Lacp    Remote System Id        Sys   Last State Changed
       Key     Lag Id                  Prio
-------------------------------------------------------------------------------
1      2       1       11:11:11:11:11:11  3     01/28/2013 12:52:38
-------------------------------------------------------------------------------
Number of LAGs : 1
===============================================================================
A:ALU-1>show>redundancy>multi-chassis#
```

```
A:ALU-1>show>redundancy>multi-chassis# mc-lag peer 10.10.10.4 statistics
===============================================================================
Multi-Chassis Statistics, Peer 10.10.10.4
===============================================================================
Packets Rx                      : 287
Packets Rx Keepalive            : 279
Packets Rx Config               : 2
Packets Rx Peer Config          : 35
Packets Rx State                : 5
Packets Dropped State Disabled  : 0
Packets Dropped Packets Too Short : 0
Packets Dropped Tlv Invalid Size  : 0
Packets Dropped Tlv Invalid LagId : 0
Packets Dropped Out of Seq      : 0
Packets Dropped Unknown Tlv     : 0
Packets Dropped MD5             : 0
Packets Tx                      : 322
Packets Tx Keepalive            : 281
Packets Tx Peer Config          : 35
Packets Tx Failed               : 0
===============================================================================
A:ALU-1>show>redundancy>multi-chassis#
```

```
A:ALU-1>show>redundancy>multi-chassis# mc-lag peer 10.10.10.4 lag 1 statistics
===============================================================================
Multi-Chassis Statistics, Peer 10.10.10.4 Lag 1
===============================================================================
Packets Rx Config               : 2
Packets Rx State                : 5
Packets Tx Config               : 1
Packets Tx State                : 5
Packets Tx Failed               : 0
===============================================================================
A:ALU-1>show>redundancy>multi-chassis#
```

Table 64: MC-LAG field descriptions

Label	Description
Last State chg	Displays date and time of the last state change for the MC-LAG peer
Admin State	Displays the administrative state of the MC-LAG peer
KeepAlive	Displays the time interval between keepalive messages exchanged between peers
Oper State	Displays the operational state of the MC-LAG peer
Hold On Ngbr Failure	Displays how many keep alive intervals the standby 7705 SAR will wait for packets from the active node before assuming a redundant neighbor node failure
Lag Id	Displays the LAG identifier, expressed as a decimal integer
Lacp Key	Displays the 16-bit Lacp key
Remote system Id	Displays the LAG identifier of the remote system, expressed as a decimal integer
Multi-Chassis Statistics	
Packets Rx	Displays the number of MC-LAG packets received from the peer
Packets Rx Keepalive	Displays the number of MC-LAG keepalive packets received from the peer
Packets Rx Config	Displays the number of MC-LAG configured packets received from the peer
Packets Rx Peer Config	Displays the number of MC-LAG packets configured by the peer
Packets Rx State	Displays the number of received MC-LAG "lag" state packets received from the peer
Packets Dropped State Disabled	Displays the number of packets that were dropped because the peer was administratively disabled
Packets Dropped Packets Too Short	Displays the number of packets that were dropped because the packet was too short
Packets Dropped Tlv Invalid Size	Displays the number of packets that were dropped because the packet size was invalid
Packets Dropped Tlv Invalid LagId	Displays the number of packets that were dropped because the packet referred to an invalid or non-multi-chassis LAG

Label	Description
Packets Dropped Out of Seq	Displays the number of packets that were dropped because the packet was out of sequence
Packets Dropped Unknown Tlv	Displays the number of packets that were dropped because the packet contained an unknown TLV
Packets Dropped MD5	Displays the number of packets that were dropped because the packet failed MD5 authentication
Packets Tx	Displays the number of packets transmitted from this system to the peer
Packets Tx Keepalive	Displays the number of keepalive packets transmitted from this system to the peer
Packets Tx Peer Config	Displays the number of configured packets transmitted from this system to the peer
Packets Tx Failed	Displays the number of packets that failed to be transmitted from this system to the peer

synchronization

Syntax

synchronization

Context

show>redundancy

Description

This command displays redundancy synchronization times.

Output

The following output is an example of redundancy synchronization information, and Table 65: Synchronization field descriptions describes the fields.

Output example

```
A:ALU-1>show>redundancy# synchronization
===============================================================================
Synchronization Information
===============================================================================
Standby Status            : disabled
Last Standby Failure      : N/A
Standby Up Time           : N/A
Failover Time             : N/A
Failover Reason           : N/A
Boot/Config Sync Mode     : None
Boot/Config Sync Status   : No synchronization
```

```
Last Config File Sync Time   : Never
Last Boot Env Sync Time      : Never
================================================================================
A:ALU-1>show>redundancy#
```

Table 65: Synchronization field descriptions

Label	Description
Standby Status	Displays the status of the standby CSM
Last Standby Failure	Displays the timestamp of the last standby failure
Standby Up Time	Displays the length of time the standby CSM has been up
Failover Time	Displays the timestamp when the last redundancy failover occurred causing a switchover from active to standby CSM. If there is no redundant CSM card in this system or no failover has occurred since the system last booted, the value will be 0.
Failover Reason	Displays a text string giving an explanation of the cause of the last redundancy failover. If no failover has occurred, an empty string displays.
Boot/Config Sync Mode	Displays the type of synchronization operation to perform between the primary and secondary CSMs after a change has been made to the configuration files or the boot environment information contained in the boot options file (BOF).
Boot/Config Sync Status	Displays the results of the last synchronization operation between the primary and secondary CSMs
Last Config File Sync Time	Displays the timestamp of the last successful synchronization of the configuration files
Last Boot Env Sync Time	Displays the timestamp of the last successful synchronization of the boot environment files

uptime

Syntax

uptime

Context

show

Description

This command displays the time since the system started.

Output

The following output is an example of system uptime information, and Table 66: System uptime field descriptions describes the fields.

Output example

```
A:ALU-1# show uptime
System Up Time          : 11 days, 18:32:02.22 (hr:min:sec)
A:ALU-1#
```

Table 66: System uptime field descriptions

Label	Description
System Up Time	The length of time the system has been up in days, hr:min:sec format

sync-if-timing

Syntax

sync-if-timing

Context

show>system

Description

This command displays synchronous interface timing operational information.

Output

The following output is an example of synchronous interface timing information, and Table 67: Sync-if-timing field descriptions describes the fields.

> **Note:** Some of the fields in the following output apply to the 7705 SAR-18 only.

Output example

```
A:ALU-1# show system sync-if-timing
===============================================================================
System Interface Timing Operational Info
===============================================================================
System Interface Timing Operational Info
===============================================================================
System Status CSM A               : Master Locked
    Reference Input Mode          : Non-revertive
    Quality Level Selection       : Disabled

Reference Order                   : bits ref1 ref2

Reference Input 1
    Admin Status                  : down
```

```
        Configured Quality Level      : none
        Rx Quality Level              : unknown
        Qualified For Use             : No
            Not Qualified Due To      : disabled
        Selected For Use              : No
            Not Selected Due To       : disabled
Reference Input 2
        Admin Status                  : down
        Configured Quality Level      : none
        Rx Quality Level              : unknown
        Qualified For Use             : No
            Not Qualified Due To      : disabled
        Selected For Use              : No
            Not Selected Due To       : disabled

Reference BITS 1
        Admin Status                  : up
        Configured Quality Level      : stu
        Rx Quality Level              : unknown
        Qualified For Use             : Yes
        Selected For Use              : Yes
        Interface Type                : DS1
        Framing                       : ESF
        Line Coding                   : B8ZS
        Output Admin Status           : up
        Output Reference Selected     : none
        Tx Quality Level              :

Reference BITS 2
        Admin Status                  : up
        Configured Quality Level      : stu
        Rx Quality Level              : unknown
        Qualified For Use             : No
            Not Qualified Due To      : LOS
        Selected For Use              : No
            Not Selected Due To       : not qualified
        Interface Type                : DS1
        Framing                       : ESF
        Line Coding                   : B8ZS
        Output Admin Status           : up
        Output Reference Selected     : none
        Tx Quality Level              :

===============================================================================
A:ALU-1#
```

Table 67: Sync-if-timing field descriptions

Label	Description
System Status CSM A	The present status of the synchronous timing equipment subsystem (SETS): • Not Present • Master Freerun • Master Holdover • Master Locked • Slave

Label	Description
	• Acquiring
Reference Input Mode	Revertive — a revalidated or a newly validated reference source that has a higher priority than the currently selected reference has reverted to the new reference source
	Non-revertive — the clock cannot revert to a higher priority clock if the current clock goes offline
Quality Level Selection	Whether Quality Level Selection is enabled or disabled
Reference Order	bits, ref1, ref2 — the priority order of the timing references
Reference Input 1, 2	The reference 1 and reference 2 input parameters
Admin Status	down — the ref1 or ref2 configuration is administratively shut down
	up — the ref1 or ref2 configuration is administratively enabled
Configured Quality Level	Synchronization Status Messaging quality level value manually configured on port for ref1 or ref2
Rx Quality Level	Synchronization Status Messaging quality level value received on port for ref1 or ref2
Qualified for Use	Whether the ref1 or ref2 timing reference is qualified for use by the synchronous timing subsystem
Selected for Use	Whether the ref1 or ref2 timing reference is presently selected
Not Selected Due To	If the ref1 or ref2 timing reference is not selected, the reason why
Not Qualified Due To	If the ref1 or ref2 timing reference is not qualified, the reason why
Source Port	None — no source port is configured or in use as a ref1 or ref2 timing reference
	card/slot/port — the source port of the ref1 or ref2 timing reference
Reference BITS 1, 2	The reference 1 and reference 2 BITS parameters, applicable to the 7705 SAR-18 only
Admin Status	down — the BITS 1 or BITS 2 configuration is administratively shut down

Label	Description
	up — the BITS 1 or BITS 2 configuration is administratively enabled
Configured Quality Level	Synchronization Status Messaging quality level value manually configured on port for BITS 1 or BITS 2
Rx Quality Level	Synchronization Status Messaging quality level value received on port for BITS 1 or BITS 2
Qualified For Use	Whether the BITS 1 or BITS 2 reference is qualified for use by the synchronous timing subsystem
Selected For Use	Whether the BITS 1 or BITS 2 reference is presently selected
Not Qualified Due To	If the BITS 1 or BITS 2 reference is not qualified, the reason why
Not Selected Due To	If the BITS 1 or BITS 2 reference is not selected, the reason why
Interface Type	The interface type for the BITS port
Framing	The framing type used by the BITS port
Line Coding	The line coding type used by the BITS port
Output Admin Status	The administrative status of the BITS output port
Output Reference Selected	The type of output reference selected by the BITS port
Tx Quality Level	The Synchronization Status Messaging quality level value transmitted on the BITS port

chassis

Syntax

chassis [**detail**]

chassis [**environment** | **power-feed**]

Context

show

Description

This command displays a summary of general chassis status information.

Parameters

detail

displays detailed information about the physical chassis

environment

displays chassis environmental status information

power-feed

displays chassis power feed status information

Output

The following output is an example of general chassis information, and Table 68: Chassis field descriptions describes the fields.

Output example

```
*A:Sar18 Dut-B# show chassis
===============================================================================
System Information
===============================================================================
  Name                              : Sar18 Dut-B
  Type                              : 7705 SAR-18
  Chassis Topology                  : Standalone
  Location                          : (Not Specified)
  Coordinates                       : (Not Specified)
  CLLI code                         :
  Number of slots                   : 3
  Oper number of slots              : 3
  Number of ports                   : 64
  Critical LED state                : Off
  Major LED state                   : Off
  Minor LED state                   : Off
  Over Temperature state            : OK
  Base MAC address                  : d6:65:ff:00:00:00
===============================================================================
Chassis Summary
===============================================================================
Chassis   Role                Status
-------------------------------------------------------------------------------
1         Standalone          up
===============================================================================
*A:Sar18 Dut-B#
```

Table 68: Chassis field descriptions

Label	Description
System Information	
Name	The system name for the router
Type	The router series model number
Chassis Topology	The chassis setup; the value is always Standalone
Location	The system location for the device

Label	Description
Coordinates	A user-configurable string that indicates the global navigation satellite system (GNSS) coordinates for the location of the chassis. For example: N 45 58 23, W 34 56 12 N37 37' 00 latitude, W122 22' 00 longitude N36 × 39.246' W121 × 40.121'
CLLI Code	The Common Language Location Identifier (CLLI) that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry
Number of slots	The number of slots in the chassis for the IOM and the CSMs, including the built-in CSMs on the fixed platforms. The IOM is a virtual slot (designated as slot 1), as it is actually a module on the CSM and does not get installed separately.
Oper number of slots	The number of slots currently operating; the value is always the same as the Number of slots value
Number of ports	The total number of ports currently installed in this chassis. This count does not include the CSM Management ports that are used for management access.
Critical LED state	The current state of the Critical LED in this chassis
Major LED state	The current state of the Major LED in this chassis
Minor LED state	The current state of the Minor LED in this chassis
Over Temperature state	Indicates whether there is an over-temperature condition
Base MAC address	The base chassis Ethernet MAC address
Chassis Summary	
Chassis	The chassis number
Role	The role of the chassis in the chassis setup; the value is always Standalone
Status	Current status of the chassis

The following output is an example of detailed chassis information, and Table 69: Chassis detail field descriptions describes the fields.

Output example

```
*A:Sar18 Dut-B# show chassis detail
```

```
===============================================================================
System Information
===============================================================================
  Name                          : Sar18 Dut-B
  Type                          : 7705 SAR-18
  Chassis Topology              : Standalone
  Location                      : (Not Specified)
  Coordinates                   : (Not Specified)
  CLLI code                     :
  Number of slots               : 3
  Oper number of slots          : 3
  Number of ports               : 64
  Critical LED state            : Off
  Major LED state               : Off
  Minor LED state               : Off
  Over Temperature state        : OK
  Base MAC address              : d6:65:ff:00:00:00
===============================================================================
Chassis 1 Detail
===============================================================================
  Chassis Status                : up
  Chassis Role                  : Standalone
  Hardware Data
    Part number                 : Sim Part#
    CLEI code                   : Sim CLEI
    Serial number               : dut-b_a
    Manufacture date            : 01012003
    Manufacturing variant       : ch1: 1471 ch2: 1491
    Time of last boot           : 2018/09/10 19:36:37
    Current alarm state         : alarm cleared
  -------------------------------------------------------------------------
Environment Information
    Fan Information
        Number of fans          : 8
        Status                  : up
        Speed                   : normal
  Hardware Data
    Part number                 : Sim Part#
    CLEI code                   : Sim CLEI
    Serial number               : fan-0
    Manufacture date            : 01012003
    Manufacturing variant       : ch1: 1471 ch2: 1491
    Time of last boot           : N/A
    Current alarm state         : alarm cleared
    Alarm Module
        Status                  : ok
        Type                    : alarm-v1
    External Alarms Interface
      ---------------------------------------------
       Input  Pin  Event         State
      ---------------------------------------------
        IN-1   1    Critical    : ok
        IN-2   2    Major       : ok
        IN-3   11   Major       : ok
        IN-4   12   Minor       : ok
      ---------------------------------------------
  Hardware Data
    Part number                 : Sim Part#
    CLEI code                   : Sim CLEI
    Serial number               : alm-mod-0
    Manufacture date            : 01012003
    Manufacturing variant       : ch1: 1471 ch2: 1491
    Time of last boot           : 2018/09/10 19:36:38
    Current alarm state         : alarm cleared
```

```
         ------------------------------------------------------------------------
Power Feed Information
       Number of power feeds         : 2
       Input power feed              : A
         Type                        : dc
         Status                      : up
       Input power feed              : B
         Type                        : dc
         Status                      : up
=========================================================================
*A:Sar18 Dut-B#
```

Table 69: Chassis detail field descriptions

Label	Description
System Information	
Name	The system name for the router
Type	The router series model number
Chassis Topology	The chassis setup; the value is always Standalone
Location	The system location for the device
Coordinates	A user-configurable string that indicates the global navigation satellite system (GNSS) coordinates for the location of the chassis. For example: N 45 58 23, W 34 56 12 N37 37' 00 latitude, W122 22' 00 longitude N36 × 39.246' W121 × 40.121'
CLLI Code	The Common Language Location Identifier (CLLI) that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry
Number of slots	The number of slots in the chassis for the IOM and the CSMs, including the built-in CSMs on the fixed platforms. The IOM is a virtual slot (designated as slot 1), as it is actually a module on the CSM and does not get installed separately.
Oper number of slots	The number of slots currently operating; the value is always the same as the Number of slots value
Number of ports	The total number of ports currently installed in this chassis. This count does not include the CSM Management ports that are used for management access.
Critical LED state	The current state of the Critical LED in this chassis

Label	Description
Major LED state	The current state of the Major LED in this chassis
Minor LED state	The current state of the Minor LED in this chassis
Over Temperature state	Indicates whether there is an over-temperature condition
Base MAC address	The base chassis Ethernet MAC address
Chassis 1 Detail	
Chassis Status	The current status of the chassis
Chassis Role	The role of the chassis in the chassis setup; the value is always Standalone
Hardware Data	Hardware information about the chassis
Part number	The CSM part number
CLEI code	The code used to identify the router
Serial number	The CSM part number; not user-modifiable
Manufacture date	The chassis manufacture date; not user-modifiable
Manufacturing variant	Factory-inputted manufacturing text string; not user-modifiable
Time of last boot	The date and time the most recent boot occurred
Current alarm state	Displays the alarm conditions for the specific board
Environment Information	
Fan information	
Number of fans	The total number of fans installed in this chassis
Status	Current status of the fans
Speed	The fan speed
Hardware Data	Hardware information for fan module
Part number	The CSM part number
CLEI code	The code used to identify the router
Serial number	The CSM part number; not user-modifiable
Manufacture date	The chassis manufacture date; not user-modifiable
Manufacturing variant	Factory-inputted manufacturing text string; not user-modifiable

Label	Description
Time of last boot	The date and time the most recent boot occurred
Current alarm state	Displays the alarm conditions for the specific board
Alarm Module	
Status	Status of the alarm module
Type	Version of the alarm module
External Alarms Interface	
Input	External alarm input number
Pin	Port connector pin number for the alarm input
Event	Severity level of events reported by this input: • Critical: critical log event, trap and critical alarm/relay LED illuminated • Major: major log event, trap and major alarm/relay LED illuminated • Minor: minor log event, trap and minor alarm/relay LED illuminated • Warning: warning log, event, trap, no alarm/relay illuminated • Indeterminate: indeterminate log event trap, no alarm/relay illuminated • Suppressed: no log events, traps or alarm/relays illuminated
Hardware Data	Hardware information for alarm module
Power Feed Information	
Number of power feeds	The number of power feeds installed in the chassis
Input power feed - Type	The type of power feed — ac power or dc power
Input power feed - Status	Up — the specified power supply is up
	Critical failure — the specified power supply has failed
	Not equipped — the specified power supply is not present
	Unknown — the software system cannot determine the type of power feed for the specified power supply
	Not monitored — the specified power supply is not monitored

The following output is an example of chassis environment information, and Table 70: Chassis environment field descriptions describes the fields.

Output example

```
*A:Sar18 Dut-B# show chassis environment
===============================================================================
Chassis 1 Detail
===============================================================================
Environment Information
    Fan Information
       Number of fans             : 8
       Status                     : up
       Speed                      : normal
Hardware Data
  Part number                     : Sim Part#
  CLEI code                       : Sim CLEI
  Serial number                   : fan-0
  Manufacture date                : 01012003
  Manufacturing variant           : ch1: 1471 ch2: 1491
  Time of last boot               : N/A
  Current alarm state             : alarm cleared
    Alarm Module
       Status                     : ok
       Type                       : alarm-v1
    External Alarms Interface
       --------------------------------------------
       Input  Pin  Event          State
       --------------------------------------------
       IN-1   1    Critical       : ok
       IN-2   2    Major          : ok
       IN-3   11   Major          : ok
       IN-4   12   Minor          : ok
       --------------------------------------------
Hardware Data
  Part number                     : Sim Part#
  CLEI code                       : Sim CLEI
  Serial number                   : alm-mod-0
  Manufacture date                : 01012003
  Manufacturing variant           : ch1: 1471 ch2: 1491
  Time of last boot               : 2018/09/10 19:36:38
  Current alarm state             : alarm cleared
===============================================================================
*A:Sar18 Dut-B#
```

Table 70: Chassis environment field descriptions

Label	Description
Environment Information	
Fan information	
Number of fans	The total number of fans installed in this chassis
Status	Current status of the fans
Speed	The fan speed
Hardware Data	Hardware information for fan module

Label	Description
Part number	The CSM part number
CLEI code	The code used to identify the router
Serial number	The CSM part number; not user-modifiable
Manufacture date	The chassis manufacture date; not user-modifiable
Manufacturing variant	Factory-inputted manufacturing text string; not user-modifiable
Time of last boot	The date and time the most recent boot occurred
Current alarm state	Displays the alarm conditions for the specific board
Alarm Module	
Status	Status of the alarm module
Type	Version of the alarm module
External Alarms Interface	
Input	External alarm input number
Pin	Port connector pin number for the alarm input
Event	Severity level of events reported by this input: • Critical: critical log event, trap and critical alarm/relay LED illuminated • Major: major log event, trap and major alarm/relay LED illuminated • Minor: minor log event, trap and minor alarm/relay LED illuminated • Warning: warning log, event, trap, no alarm/relay illuminated • Indeterminate: indeterminate log event trap, no alarm/relay illuminated • Suppressed: no log events, traps or alarm/relays illuminated
State	State of alarm event
Hardware data	Hardware information for alarm module

The following output is an example of chassis power feed information, and Table 71: Chassis power feed field descriptions describes the fields.

Output example

```
*A:Sar18 Dut-B# show chassis power-feed
===============================================================================
System Information
===============================================================================
```

```
    Name                            : Sar18 Dut-B
    Type                            : 7705 SAR-18
    Chassis Topology                : Standalone
    Location                        : (Not Specified)
    Coordinates                     : (Not Specified)
    CLLI code                       :
    Number of slots                 : 3
    Oper number of slots            : 3
    Number of ports                 : 64
    Critical LED state              : Off
    Major LED state                 : Off
    Minor LED state                 : Off
    Over Temperature state          : OK
    Base MAC address                : d6:65:ff:00:00:00
===============================================================================
Chassis 1 Detail
===============================================================================
    Chassis Status                  : up
    Chassis Role                    : Standalone
    Hardware Data
      Part number                   : Sim Part#
      CLEI code                     : Sim CLEI
      Serial number                 : dut-b_a
      Manufacture date              : 01012003
      Manufacturing variant         : ch1: 1471 ch2: 1491
      Time of last boot             : 2018/09/10 19:36:37
      Current alarm state           : alarm cleared
    -------------------------------------------------------------------------
Power Feed Information
        Number of power feeds       : 2
        Input power feed            : A
          Type                      : dc
          Status                    : up
        Input power feed            : B
          Type                      : dc
          Status                    : up
===============================================================================
*A:Sar18 Dut-B# show chassis power-feed
```

Table 71: Chassis power feed field descriptions

Label	Description
System Information	
Name	The system name for the router
Type	The router series model number
Chassis Topology	The chassis setup; the value is always Standalone
Location	The system location for the device
Coordinates	A user-configurable string that indicates the global navigation satellite system (GNSS) coordinates for the location of the chassis. For example: N 45 58 23, W 34 56 12

Label	Description
	N37 37' 00 latitude, W122 22' 00 longitude N36 × 39.246' W121 × 40.121'
CLLI Code	The Common Language Location Identifier (CLLI) that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry
Number of slots	The number of slots in the chassis for the IOM and the CSMs, including the built-in CSMs on the fixed platforms. The IOM is a virtual slot (designated as slot 1), as it is actually a module on the CSM and does not get installed separately.
Oper number of slots	The number of slots currently operating; the value is always the same as the Number of slots value
Number of ports	The total number of ports currently installed in this chassis. This count does not include the CSM Management ports that are used for management access.
Critical LED state	The current state of the Critical LED in this chassis
Major LED state	The current state of the Major LED in this chassis
Minor LED state	The current state of the Minor LED in this chassis
Over Temperature state	Indicates whether there is an over-temperature condition
Base MAC address	The base chassis Ethernet MAC address
Chassis 1 Detail	
Chassis Status	Current status of the chassis
Chassis Role	The role of the chassis in the chassis setup; the value is always Standalone
Hardware Data	Hardware information about the chassis
Part number	The CSM part number
CLEI code	The code used to identify the router
Serial number	The CSM part number; not user-modifiable
Manufacture date	The chassis manufacture date; not user-modifiable
Manufacturing variant	Factory-inputted manufacturing text string; not user-modifiable
Time of last boot	The date and time the most recent boot occurred
Current alarm state	Displays the alarm conditions for the specific board

Label	Description
Power Feed Information	
Number of power feeds	The number of power feeds
Input power feed - Type	The type of power feed — ac power or dc power
Input power feed - Status	Up — the specified power supply is up
	Critical failure — the specified power supply has failed
	Not equipped — the specified power supply is not present
	Unknown — the software system cannot determine the type of power feed for the specified power supply
	Not monitored — the specified power supply is not monitored

6.13.2.4 Clear Commands

screen

Syntax

screen

Context

clear

Description

This command allows an operator to clear the Telnet or console screen.

ptp

Syntax

ptp

Context

clear>system

Description

This command enables the context to clear Precision Timing Protocol (PTP) information.

clock

Syntax

clock *clock-id* **statistics**

clock csm port *port-id* **statistics**

Context

clear>system>ptp

Description

This command clears PTP clock information.

Parameters

clock-id

specifies the clock ID of this PTP instance

> **Values**   1 to 16 for PTP clocks that use IPv4 encapsulation
>
> **csm** for a PTP clock that uses Ethernet encapsulation

port-id

specifies a PTP Ethernet port in the format *slot/mda/port*

statistics

clears statistics on the PTP clock or Ethernet port

script-control

Syntax

script-control

Context

clear>system

Description

This command enables the context to clear script information.

script-policy

Syntax

script-policy

Context

clear>system>script-control

Description

This command enables the context to clear script policy information.

completed

Syntax

completed [*policy-name*] [**owner** *policy-owner*]

Context

clear>system>script-control>script-policy

Description

This command clears completed script run history entries.

Parameters

policy-name

specifies to only clear history entries for the specified script policy

owner-name

specifies to only clear history entries for script policies with the specified owner

sync-if-timing

Syntax

sync-if-timing {**external** | **ref1** | **ref2**}

Context

clear>system

Description

This command allows an operator to individually clear (re-enable) a previously failed reference. As long as the reference is one of the valid options, this command is always executed. An inherent behavior enables the revertive mode which causes a re-evaluation of all available references.

Parameters

external

clears the third timing reference

ref1

clears the first timing reference

ref2

        clears the second timing reference

trace

Syntax
trace log

Context
clear

Description
This command allows an operator to clear the trace log.

6.13.2.5 Debug Commands

sync-if-timing

Syntax
sync-if-timing

Context
debug

Description
This command enables the context to debug synchronous interface timing references.

force-reference

Syntax
force-reference {external | ref1 | ref2}
no force-reference

Context
debug>sync-if-timing

Description
This command allows an operator to force the system synchronous timing output to use a specific reference.

Note: This command should be used for testing and debugging purposes only. Once the system timing reference input has been forced, it will not revert to another reference at any time. The state of this command is not persistent between system boots.

When the **debug force-reference** command is executed, the current system synchronous timing output is immediately referenced from the specified reference input. If the specified input is not available (shutdown), or in a disqualified state, the timing output will enter the holdover state based on the previous input reference.

Parameters

ref1

forces the clock to use the first timing reference

ref2

forces the clock to use the second timing reference

external

forces the clock to use the third timing reference

system

Syntax

[**no**] **system**

Context

debug

Description

This command displays system debug information.

http-connections

Syntax

http-connections [*host-ip-address/mask*]

no http-connections

Context

debug>system

Description

This command displays HTTP connections debug information.

Parameters

host-ip-address/mask

displays information for the specified host IP address and mask

ntp

Syntax

ntp router *router-name* **interface** *ip-int-name*

no ntp

Context

debug>system

Description

This command enables and configures debugging for NTP.

The **no** form of the command disables debugging for NTP.

Parameters

router-name

specifies the route name, either base or management

Default   base

ip-int-name

maximum 32 characters; must begin with a letter. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

lag

Syntax

lag [**lag-id** *lag-id* [**port** *port-id*]] [**all**]

lag [**lag-id** *lag-id* [**port** *port-id*]] [**sm**] [**pkt**] [**cfg**] [**red**] [**iom-upd**] [**port-state**] [**timers**] [**sel-logic**] [**mc**] [**mc-pkt**]

no lag [**lag-id** *lag-id*]

Context

debug

Description

This command enables debugging for a LAG.

The **no** form of the command disables debugging for a LAG.

Parameters

lag-id

specifies the LAG identifier, expressed as a decimal integer

Values   1 to 32

port-id

specifies the physical port ID in the *slot/mda/port* format

all

traces all LAG and LACP parameters

sm

traces the LACP state machine

pkt

traces LACP packets

cfg

traces the LAG configuration

red

traces the LAG high availability

iom-upd

traces LAG IOM updates

port-state

traces LAG port state transitions

timers

traces LAG timers

sel-logic

traces LACP selection logic

mc

traces multi-chassis parameters

mc-pkt

traces received MC-LAG control packets with valid authentication

7 List of acronyms

Table 72: Acronyms

Acronym	Expansion
2G	second-generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third-generation mobile telephone technology
6VPE	IPv6 on Virtual Private Edge Router
7705 SAR	7705 Service Aggregation Router
7750 SR	7750 Service Router
8 PSK	eight phase shift keying
16 QAM	16-state quadrature amplitude modulation
32 QAM	32-state quadrature amplitude modulation
64 QAM	64-state quadrature amplitude modulation
128 QAM	128-state quadrature amplitude modulation
256 QAM	256-state quadrature amplitude modulation
ABR	area border router available bit rate
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
AD	auto-discovery
ADM	add/drop multiplexer
ADP	automatic discovery protocol
AES	advanced encryption standard
AFI	authority and format identifier

Acronym	Expansion
AIGP	accumulated IGP
AIS	alarm indication signal
ALG	application level gateway
AMP	active multipath
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system
ASAP	any service, any port
ASBR	autonomous system boundary router
ASM	any-source multicast autonomous system message
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
AU	administrative unit
AUG	administrative unit group
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
BBE	background block errors
Bc	committed burst size
Be	excess burst size
BECN	backward explicit congestion notification
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection

Acronym	Expansion
BGP	border gateway protocol
BGP-LS	border gateway protocol link state
BGP-LU	border gateway protocol labeled unicast
BITS	building integrated timing supply
BTCA	best timeTransmitter clock algorithm
BMU	broadcast, multicast, and unknown traffic Traffic that is not unicast. Any nature of multipoint traffic: • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BNM	bandwidth notification message
BOF	boot options file
BoS	bottom of stack
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSM	bootstrap message
BSR	bootstrap router
BSTA	Broadband Service Termination Architecture
BTS	base transceiver station
CA	certificate authority
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space

Acronym	Expansion
CC	continuity check control channel
CCM	continuity check message
CCTV	closed-circuit television
CE	circuit emulation customer edge
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
cHDLC	Cisco high-level data link control protocol
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CMP	certificate management protocol
C-multicast	customer multicast
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPROTO	C prototype
CPU	central processing unit
C/R	command/response
CRC	cyclic redundancy check
CRC-32	32-bit cyclic redundancy check

Acronym	Expansion
CRL	certificate revocation list
CRON	a time-based scheduling service (from chronos = time)
CRP	candidate RP
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-tag	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
CWDM	coarse wavelength-division multiplexing
DA/FAN	distribution automation and field area network
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DCR	differential clock recovery
DDoS	distributed DoS
DE	discard eligibility
DER	distinguished encoding rules
DES	data encryption standard
DF	do not fragment designated forwarder
DH	Diffie-Hellman
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6

Acronym	Expansion
DIS	designated intermediate system
DLCI	data link connection identifier
DLCMI	data link connection management interface
DM	delay measurement
DNS	domain name server
DNU	do not use
DoS	denial of service
dot1p	IEEE 802.1p bits, in Ethernet or VLAN ingress packet headers, used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPD	dead peer detection
DPI	deep packet inspection
DPLL	digital phase locked loop
DR	designated router
DSA	digital signal algorithm
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DUS	do not use for synchronization
DV	delay variation
DVMRP	distance vector multicast routing protocol
e911	enhanced 911 service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)

Acronym	Expansion
E-BSR	elected BSR
ECMP	equal cost multipath
EE	end entity
EFM	Ethernet in the first mile
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
EIR	excess information rate
EJBCA	Enterprise Java Bean Certificate Authority
E-LAN	Ethernet local area network
E-Line	Ethernet virtual private line
EL	entropy label
eLER	egress label edge router
ELI	entropy label indicator
E&M	ear and mouth earth and magneto exchange and multiplexer
eMBMS	evolved MBMS
EOP	end of packet
EPC	evolved packet core
EPD	early packet discard
Epipe	Ethernet VLL
EPL	Ethernet private line
EPON	Ethernet Passive Optical Network
EPS	equipment protection switching
ERO	explicit route object
ES	Ethernet segment errored seconds

Acronym	Expansion
ESD	electrostatic discharge
ESI	Ethernet segment identifier
ESMC	Ethernet synchronization message channel
ESN	extended sequence number
ESP	encapsulating security payload
ESPI	encapsulating security payload identifier
ETE	end-to-end
ETH-BN	Ethernet bandwidth notification
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVC	Ethernet virtual connection
EVDO	evolution - data optimized
EVI	EVPN instance
EVPL	Ethernet virtual private link
EVPN	Ethernet virtual private network
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FD	frequency diversity
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FECN	forward explicit congestion notification
FeGW	far-end gateway
FEP	front-end processor
FF	fixed filter
FFD	fast fault detection

Acronym	Expansion
FIB	forwarding information base
FIFO	first in, first out
FIPS-140-2	Federal Information Processing Standard publication 140-2
FM	fault management
FNG	fault notification generator
FOM	figure of merit
Fpipe	frame relay VLL
FQDN	fully qualified domain name
FR	frame relay
FRG bit	fragmentation bit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
FXO	foreign exchange office
FXS	foreign exchange subscriber
GFP	generic framing procedure
GigE	Gigabit Ethernet
GLONASS	Global Navigation Satellite System (Russia)
GNSS	global navigation satellite system (generic)
GPON	Gigabit Passive Optical Network
GPRS	general packet radio service
GPS	Global Positioning System
GRE	generic routing encapsulation
GRT	global routing table
GSM	Global System for Mobile Communications (2G)
GTP-U	GPRS tunneling protocol user plane
GW	gateway

Acronym	Expansion
HA	high availability
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HDLC	high-level data link control protocol
HEC	header error control
HMAC	hash message authentication code
Hpipe	HDLC VLL
H-QoS	hierarchical quality of service
HSB	hot standby
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
H-VPLS	hierarchical virtual private line service
IANA	Internet Assigned Numbers Authority
IBN	isolated bonding networks
ICB	inter-chassis backup
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
IDS	intrusion detection system
IDU	indoor unit
IED	intelligent end device
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
IGMP	Internet group management protocol
IGP	interior gateway protocol

Acronym	Expansion
IID	instance ID
IKE	Internet key exchange
iLER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IMET-IR	inclusive multicast Ethernet tag—ingress replication
INVARP	inverse address resolution protocol
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
I-PMSI	inclusive PMSI
IPoATM	IP over ATM
IPS	intrusion prevention system
IPSec	Internet Protocol security
IR	ingress replication
IRB	integrated routing and bridging
ISA	integrated services adapter
ISAKMP	Internet security association and key management protocol
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization
IW	interworking
JP	join prune
KG	key group
LB	loopback

Acronym	Expansion
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LFA	loop-free alternate
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LMI	local management interface
LOS	line-of-sight loss of signal
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSPA	LSP attributes
LSR	label switch router link-state request
LSU	link-state update
LT	linktrace
LTE	long term evolution

Acronym	Expansion
	line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE
LTR	link trace reply
MA	maintenance association
MAC	media access control
MA-ID	maintenance association identifier
MBB	make-before-break
MBGP	multicast BGP multiprotocol BGP multiprotocol extensions for BGP
MBMS	multimedia broadcast multicast service
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MCAC	multicast connection admission control
MC-APS	multi-chassis automatic protection switching
MC-MLPPP	multi-class multilink point-to-point protocol
MCS	multicast server multi-chassis synchronization
MCT	MPT craft terminal
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDB	multidrop data bridge
MDL	maintenance data link
MDT	multicast distribution tree
ME	maintenance entity

Acronym	Expansion
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification
MHD	multi-homed device
MHF	MIP half function
MHN	multi-homed network
MIB	management information base
MI-IS-IS	multi-instance IS-IS
MIR	minimum information rate
MLD	multicast listener discovery
mLDP	multicast LDP
MLPPP	multilink point-to-point protocol
mLSP	multicast LSP
MoFRR	multicast-only fast reroute
MP	merge point multilink protocol multipoint
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPLSCP	multiprotocol label switching control protocol
MPP	MPT protection protocol
MPR	see Wavence
MPR-e	Microwave Packet Radio (standalone mode)
MPT-HC V2/9558HC	Microwave Packet Transport, High Capacity version 2

Acronym	Expansion
MPT-HLC	Microwave Packet Transport, High-Capacity Long-Haul Cubic (ANSI)
MPT-HQAM	Microwave Packet Transport, High Capacity (MPT-HC-QAM) or Extended Power (MPT-XP-QAM) with 512/1024 QAM
MPT-MC	Microwave Packet Transport, Medium Capacity
MPT-XP	Microwave Packet Transport, High Capacity (very high power version of MPT-HC V2/9558HC)
MRAI	minimum route advertisement interval
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDP	Multicast Source Discovery Protocol
MSDU	MAC Service Data Unit
MSO	multi-system operator
MS-PW	multi-segment pseudowire
MSS	maximum segment size Microwave Service Switch
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
M-VPLS	management virtual private line service
MVPN	multicast VPN
MVR	multicast VPLS registration
MW	microwave
MWA	microwave awareness
N·M	newton meter
NAT	network address translation
NAT-T	network address translation traversal
NBMA	non-broadcast multiple access (network)

Acronym	Expansion
ND	neighbor discovery
NE	network element
NET	network entity title
NFM-P	Network Functions Manager - Packet (formerly 5620 SAM)
NGE	network group encryption
NG-MVPN	next generation MVPN
NH	next hop
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLOS	non-line-of-sight
NLPID	network level protocol identifier
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NOC	network operations center
NPAT	network port address translation
NRC-F	Network Resource Controller - Flow
NRC-P	Network Resource Controller - Packet
NRC-T	Network Resource Controller - Transport
NRC-X	Network Resource Controller - Cross Domain
NSAP	network service access point
NSD	Network Services Director
NSP	native service processing Network Services Platform
NSSA	not-so-stubby area
NTP	network time protocol

Acronym	Expansion
NTR	network timing reference
OADM	optical add/drop multiplexer
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier level 3
OCSP	online certificate status protocol
ODU	outdoor unit
OIF	outgoing interface
OLT	optical line termination
OMC	optical management console
ONT	optical network terminal
OOB	out-of-band
OPX	off premises extension
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	open shortest path first
OSPF-TE	OSPF-traffic engineering (extensions)
OSS	operations support system
OSSP	organization specific slow protocol
OTP	one time password
OWAMP	one-way active measurement protocol
P2MP	point to multipoint
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities

Acronym	Expansion
PSB	path state block
PBO	packet byte offset
PBR	policy-based routing
PBX	private branch exchange
PCAP	packet capture
PCC	Path Computation Element Client
PCE	Path Computation Element
PCEP	Path Computation Element Protocol
PCM	pulse code modulation
PCP	priority code point
PCR	proprietary clock recovery
PDU	power distribution unit protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PEAPv0	protected extensible authentication protocol version 0
PEM	privacy enhanced mail
PFoE	power feed over Ethernet
PFS	perfect forward secrecy
PHB	per-hop behavior
PHP	penultimate hop popping
PHY	physical layer
PIC	prefix independent convergence
PID	protocol ID
PIM SSM	protocol independent multicast—source-specific multicast
PIR	peak information rate
PKCS	public key cryptography standards

Acronym	Expansion
PKI	public key infrastructure
PLAR	private line automatic ringdown
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
PLSP	path LSP
PM	performance monitoring
PMSI	P-multicast service interface
P-multicast	provider multicast
PoE	power over Ethernet
PoE+	power over Ethernet plus
POH	path overhead
POI	purge originator identification
PoP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PPS	pulses per second
PRC	primary reference clock
PRS	primary reference source
PRTC	primary reference time clock
PSE	power sourcing equipment
PSK	pre-shared key
PSN	packet switched network
PSNP	partial sequence number PDU
PTA	PMSI tunnel attribute
PTM	packet transfer mode
PTP	performance transparency protocol precision time protocol

Acronym	Expansion
PuTTY	an open-source terminal emulator, serial console, and network file transfer application
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
Q.922	ITU-T Q-series Specification 922
QL	quality level
QoS	quality of service
QPSK	quadrature phase shift keying
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication
RED	random early discard
RESV	reservation
RIB	routing information base
RIP	routing information protocol
RJ45	registered jack 45
RMON	remote network monitoring
RNC	Radio Network Controller
RP	rendezvous point
RPF RTM	reverse path forwarding RTM
RPS	radio protection switching
RPT	rendezvous-point tree
RR	route reflector

Acronym	Expansion
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSA	Rivest, Shamir, and Adleman (authors of the RSA encryption algorithm)
RSHG	residential split horizon group
RSTP	rapid spanning tree protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit
RTC	route target constraint
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
r-VPLS	routed virtual private LAN service
SA	security association source-active
SAA	service assurance agent
SAFI	subsequent address family identifier
SAP	service access point
SAToP	structure-agnostic TDM over packet
SCADA	surveillance, control and data acquisition
SC-APS	single-chassis automatic protection switching
SCP	secure copy
SCTP	Stream Control Transmission Protocol
SD	signal degrade space diversity

Acronym	Expansion
SDH	synchronous digital hierarchy
SDI	serial data interface
SDN	software defined network
SDP	service destination point
SE	shared explicit
SeGW	secure gateway
SES	severely errored seconds
SETS	synchronous equipment timing source
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SFTP	SSH file transfer protocol
(S,G)	(source, group)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate
SLA	Service Level Agreement
SLARP	serial line address resolution protocol
SLID	subscriber location identifier of a GPON module
SLM	synthetic loss measurement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNR	signal to noise ratio
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first

Acronym	Expansion
SPI	security parameter index
S-PMSI	selective PMSI
SPT	shortest path tree
SR	service router (7750 SR) segment routing
SRLG	shared risk link group
SRP	stateful request parameter
SRRP	subscriber routed redundancy protocol
SR-ISIS	segment routing IS-IS
SR-OSPF	segment routing OSPF
SR-TE	segment routing traffic engineering
SSH	secure shell
SSM	source-specific multicast synchronization status messaging
SSU	system synchronization unit
S-tag	service VLAN tag
STM	synchronous transport module
STM1	synchronous transport module, level 1
STP	spanning tree protocol
STS	synchronous transport signal
SVC	switched virtual circuit
SVEC	synchronization vector
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
TDA	transmit diversity antenna
TDEV	time deviation

Acronym	Expansion
TDM	time division multiplexing
TE	traffic engineering
TEDB	traffic engineering database
TEID	tunnel endpoint identifier
TEP	tunnel endpoint
TFTP	trivial file transfer protocol
T-LDP	targeted LDP
TLS	transport layer security
TLV	type length value
TM	traffic management
ToD	time of day
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier
TPIF	IEEE C37.94 teleprotection interface
TPMR	two-port MAC relay
TPS	transmission protection switching
TSoP	Transparent SDH/SONET over Packet
TTL	time to live
TTLS	tunneled transport layer security
TTM	tunnel table manager
TU	tributary unit
TUG	tributary unit group
TWAMP	two-way active measurement protocol
U-APS	unidirectional automatic protection switching
UAS	unavailable seconds
UBR	unspecified bit rate

Acronym	Expansion
UDP	user datagram protocol
UFD	unidirectional forwarding detection
UMH	upstream multicast hop
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
uRPF	unicast reverse path forwarding
V.11	ITU-T V-series Recommendation 11
V.24	ITU-T V-series Recommendation 24
V.35	ITU-T V-series Recommendation 35
VC	virtual circuit
VCB	voice conference bridge
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VM	virtual machine
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VPWS	virtual private wire service

Acronym	Expansion
VRF	virtual routing and forwarding table
VRRP	virtual router redundancy protocol
V-SAP	virtual service access point
VSE	vendor-specific extension
VSI	virtual switch instance
VSO	vendor-specific option
VT	virtual trunk virtual tributary
VTG	virtual tributary group
Wavence	formerly 9500 MPR (Microwave Packet Radio)
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard
WTR	wait to restore
X.21	ITU-T X-series Recommendation 21
XOR	exclusive-OR
XRO	exclude route object

8 Supported standards and protocols

This chapter lists the 7705 SAR compliance with security and telecom standards, the protocols supported, and proprietary MIBs.

8.1 Security standards

FIPS 140-2—Federal Information Processing Standard publication 140-2, Security Requirements for Cryptographic Modules

8.2 Telecom standards

ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks

IEEE 802.1ag—Service Layer OAM

IEEE 802.1p/q—VLAN Tagging

IEEE 802.3—10BaseT

IEEE 802.3ab—1000BaseT

IEEE 802.3ah—Ethernet OAM

IEEE 802.3u—100BaseTX

IEEE 802.3x —Flow Control

IEEE 802.3z—1000BaseSX/LX

IEEE 802.3-2008—Revised base standard

IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)

IEEE C37.94-2017—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment

ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)

ITU-T G.826—End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

ITU-T G.8032 — Ethernet Ring Protection Switching

ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics

ITU-T Y.1564—Ethernet service activation test methodology

ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

8.3 Protocol support

8.3.1 ATM

AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)

af-tm-0121.000—Traffic Management Specification Version 4.1, March 1999

GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996

ITU-T Recommendation I.432.1—B-ISDN user-network interface - Physical layer specification: General characteristics

ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95

RFC 2514—Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999

RFC 2515—Definition of Managed Objects for ATM Management, February 1999

RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5

8.3.2 BFD

RFC 7130—Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces

RFC 7881—Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS

draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base

draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection

draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)

draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

8.3.3 BGP

RFC 1397—BGP Default Route Advertisement

RFC 1997—BGP Communities Attribute

RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option

RFC 2439—BGP Route Flap Dampening

RFC 2545—Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing

RFC 2918—Route Refresh Capability for BGP-4

RFC 3107—Carrying Label Information in BGP-4

RFC 3392—Capabilities Advertisement with BGP-4

RFC 4271—BGP-4 (previously RFC 1771)

RFC 4360—BGP Extended Communities Attribute

RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)

RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)

RFC 4486—Subcodes for BGP Cease Notification Message

RFC 4684—Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)

RFC 4724—Graceful Restart Mechanism for BGP - GR Helper

RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)

RFC 4893—BGP Support for Four-octet AS Number Space

RFC 6513—Multicast in MPLS/BGP IP VPNs

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

RFC 7311—The Accumulated IGP Metric Attribute for BGP

RFC 7606—Revised Error Handling for BGP UPDATE Messages

draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP

draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of Multiple Paths in BGP

8.3.4 DHCP/DHCPv6

RFC 1534—Interoperation between DHCP and BOOTP

RFC 2131—Dynamic Host Configuration Protocol (REV)

RFC 2132—DHCP Options and BOOTP Vendor Extensions

RFC 3046—DHCP Relay Agent Information Option (Option 82)

RFC 3315—Dynamic Host Configuration Protocol for IPv6

RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

8.3.5 Differentiated Services

RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers

RFC 2597—Assured Forwarding PHB Group

RFC 2598—An Expedited Forwarding PHB

RFC 3140—Per-Hop Behavior Identification Codes

8.3.6 Digital data network management

V.35

RS-232 (also known as EIA/TIA-232)

X.21

8.3.7 ECMP

RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

8.3.8 Ethernet VPN (EVPN)

RFC 7432—BGP MPLS-Based Ethernet VPN

draft-ietf-bess-evpn-vpls-seamless-integ—(PBB-)EVPN Seamless Integration with (PBB-)VPLS

draft-ietf-bess-evpn-vpws—Virtual Private Wire Service support in Ethernet VPN

draft-ietf-rabadan-bess-evpn-pref-pdf—Preference-based EVPN DF Election

8.3.9 Frame Relay

ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service

ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer - ISDN data link layer specification for frame mode bearer services

FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement

RFC 2427—Multiprotocol Interconnect over Frame Relay

8.3.10 GRE

RFC 2784—Generic Routing Encapsulation (GRE)

8.3.11 Internet Protocol (IP) – Version 4

RFC 768—User Datagram Protocol

RFC 791—Internet Protocol

RFC 792—Internet Control Message Protocol

RFC 793—Transmission Control Protocol

RFC 826—Ethernet Address Resolution Protocol

RFC 854—Telnet Protocol Specification

RFC 1350—The TFTP Protocol (Rev. 2)

RFC 1812—Requirements for IPv4 Routers

RFC 3021—Using 31-Bit Prefixes on IPv4 Point-to-Point Links

8.3.12 Internet Protocol (IP) – Version 6

RFC 2460—Internet Protocol, Version 6 (IPv6) Specification

RFC 2462—IPv6 Stateless Address Autoconfiguration

RFC 2464—Transmission of IPv6 Packets over Ethernet Networks

RFC 3587—IPv6 Global Unicast Address Format

RFC 3595—Textual Conventions for IPv6 Flow Label

RFC 4007—IPv6 Scoped Address Architecture

RFC 4193—Unique Local IPv6 Unicast Addresses

RFC 4291—IPv6 Addressing Architecture

RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 4649—DHCPv6 Relay Agent Remote-ID Option

RFC 4861—Neighbor Discovery for IP version 6 (IPv6)

RFC 5095—Deprecation of Type 0 Routing Headers in IPv6

RFC 5952—A Recommendation for IPv6 Address Text Representation

8.3.13 IPSec

ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

PKCS #12 Personal Information Exchange Syntax Standard

RFC 2315—PKCS #7: Cryptographic Message Syntax

RFC 2409—The Internet Key Exchange (IKE)

RFC 2986—PKCS #10: Certification Request Syntax Specification

RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

RFC 3947—Negotiation of NAT-Traversal in the IKE

RFC 3948—UDP Encapsulation of IPsec ESP Packets

RFC 4301—Security Architecture for the Internet Protocol

RFC 4303—IP Encapsulating Security Payload (ESP)

RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 7383—Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation

8.3.14 IS-IS

RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)

RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments

RFC 2763—Dynamic Hostname Exchange for IS-IS

RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS

RFC 2973—IS-IS Mesh Groups

RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

RFC 3567—Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

RFC 3719—Recommendations for Interoperable Networks using IS-IS

RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)

RFC 3787—Recommendations for Interoperable IP Networks

RFC 4205 for Shared Risk Link Group (SRLG) TLV

RFC 4971—Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information

RFC 5120—M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)

RFC 5304—IS-IS Cryptographic Authentication

RFC 5305—IS-IS Extensions for Traffic Engineering

RFC 5307—IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)

RFC 5308—Routing IPv6 with IS-IS

RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols

RFC 5310—IS-IS Generic Cryptographic Authentication

RFC 6232—Purge Originator Identification TLV for IS-IS

8.3.15 LDP

RFC 5036—LDP Specification

RFC 5283—LDP Extension for Inter-Area Label Switched Paths

RFC 5350—-IANA Considerations for the IPv4 and IPv6 Router Alert Options

RFC 5443—LDP IGP Synchronization

RFC 5561—LDP Capabilities

RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root

RFC 6829—Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6

RFC 7552—Updates to LDP for IPv6

draft-ietf-mpls-ldp-ip-pw-capability—Controlling State Advertisements Of Non-negotiated LDP Applications

draft-ietf-mpls-oam-ipv6-rao—IPv6 Router Alert Option for MPLS OAM

draft-pdutta-mpls-ldp-adj-capability-00—LDP Adjacency Capabilities

draft-pdutta-mpls-ldp-v2-00—LDP Version 2

draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multi-point LDP Tunnels

8.3.16 LDP and IP FRR

RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

RFC 7490—Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)

8.3.17 MPLS

RFC 3031—MPLS Architecture

RFC 3032—MPLS Label Stack Encoding

RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)

RFC 5440—Path Computation Element (PCE) Communication Protocol (PCEP)

RFC 6790—The Use of Entropy Labels in MPLS Forwarding

RFC 8253—PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)

RFC 8697—Path Computation Element Communication Protocol (PCEP) Extensions for Establishing Relationships between Sets of Label Switched Paths (LSPs)

RFC 8745—Path Computation Element Communication Protocol (PCEP) Extensions for Associating Working and Protection Label Switched Paths (LSPs) with Stateful PCE

RFC 8800—Path Computation Element Communication Protocol (PCEP) Extension for Label Switched Path (LSP) Diversity Constraint Signaling

draft-dhody-pce-pceps-tls13-02—Updates for PCEPS

draft-ietf-pce-stateful-pce—PCEP Extensions for Stateful PCE

draft-ietf-pce-segment-routing—PCEP Extensions for Segment Routing

draft-alvarez-pce-path-profiles—PCE Path Profiles

8.3.18 MPLS – OAM

RFC 6424— Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

RFC 8029—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

8.3.19 Multicast

RFC 3956—Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

RFC 3973—Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

RFC 4610—Anycast-RP Using Protocol Independent Multicast (PIM), which is similar to RFC 3446—Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs

RFC 6826—Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

cisco-ipmulticast/pim-autorp-spec—Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast, which is similar to RFC 5059—Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)

draft-ietf-mboned-msdp-deploy-nn.txt—Multicast Source Discovery Protocol (MSDP) Deployment Scenarios

8.3.20 Network Management

IANA-IFType-MIB

ITU-T X.721—Information technology- OSI-Structure of Management Information

ITU-T X.734—Information technology- OSI-Systems Management: Event Report Management Function

M.3100/3120—Equipment and Connection Models

RFC 1157—SNMPv1

RFC 1850—OSPF-MIB

RFC 1907—SNMPv2-MIB

RFC 2011—IP-MIB

RFC 2012—TCP-MIB

RFC 2013—UDP-MIB

RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

RFC 2096—IP-FORWARD-MIB

RFC 2138—RADIUS

RFC 2206—RSVP-MIB

RFC 2571—SNMP-FRAMEWORKMIB

RFC 2572—SNMP-MPD-MIB

RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB

RFC 2574—SNMP-USER-BASED-SMMIB

RFC 2575—SNMP-VIEW-BASED ACM-MIB

RFC 2576—SNMP-COMMUNITY-MIB

RFC 2588—SONET-MIB

RFC 2665—EtherLike-MIB

RFC 2819—RMON-MIB

RFC 2863—IF-MIB

RFC 2864—INVERTED-STACK-MIB

RFC 3014—NOTIFICATION-LOG MIB

RFC 3164—The BSD Syslog Protocol

RFC 3273—HCRMON-MIB

RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413—Simple Network Management Protocol (SNMP) Applications

RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3418—SNMP MIB

RFC 3954—Cisco Systems NetFlow Services Export Version 9

RFC 5101—Specification of the IP Flow Information Export (IPFIX) Protocol

for the Exchange of IP Traffic Flow Information

RFC 5102—Information Model for IP Flow Information Export

draft-ietf-disman-alarm-mib-04.txt

draft-ietf-mpls-ldp-mib-07.txt

draft-ietf-ospf-mib-update-04.txt

draft-ietf-mpls-lsr-mib-06.txt

draft-ietf-mpls-te-mib-04.txt

TMF 509/613—Network Connectivity Model

8.3.21 OSPF

RFC 1765—OSPF Database Overflow

RFC 2328—OSPF Version 2

RFC 2370—Opaque LSA Support

RFC 2740—OSPF for IPv6

RFC 3101—OSPF NSSA Option

RFC 3137—OSPF Stub Router Advertisement

RFC 3509—Alternative Implementations of OSPF Area Border Routers

RFC 3623—Graceful OSPF Restart (support for Helper mode)

RFC 3630—Traffic Engineering (TE) Extensions to OSPF

RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

RFC 4915—Multi-Topology (MT) Routing in OSPF

RFC 4970—Extensions to OSPF for Advertising Optional Router Capabilities

RFC 5185—OSPF Multi-Area Adjacency

8.3.22 OSPFv3

RFC 4552—Authentication/Confidentiality for OSPFv3

8.3.23 PPP

RFC 1332—PPP Internet Protocol Control Protocol (IPCP)

RFC 1570—PPP LCP Extensions

RFC 1619—PPP over SONET/SDH

RFC 1661—The Point-to-Point Protocol (PPP)

RFC 1662—PPP in HDLC-like Framing

RFC 1989—PPP Link Quality Monitoring

RFC 1990—The PPP Multilink Protocol (MP)

RFC 2686—The Multi-Class Extension to Multi-Link PPP

8.3.24 Pseudowires

Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks

RFC 3550—RTP: A Transport Protocol for Real-Time Applications

RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture

RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

RFC 4446—IANA Allocation for PWE3

RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks

RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks

RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks

RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks

RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service

RFC 5085—Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RFC 5086—Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

8.3.25 RIP

RFC 1058—Routing Information Protocol

RFC 2453—RIP Version 2

8.3.26 RADIUS

RFC 2865—Remote Authentication Dial In User Service

RFC 2866—RADIUS Accounting

8.3.27 RSVP-TE and FRR

RFC 2430—A Provider Architecture for DiffServ & TE

RFC 2702—Requirements for Traffic Engineering over MPLS

RFC 2747—RSVP Cryptographic Authentication

RFC 2961—RSVP Refresh Overhead Reduction Extensions

RFC 3097—RSVP Cryptographic Authentication - Updated Message Type Value

RFC 3209—Extensions to RSVP for LSP Tunnels

RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels

RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)

RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels

8.3.28 Segment Routing (SR)

draft-francois-rtgwg-segment-routing-ti-lfa-04—Topology Independent Fast Reroute using Segment Routing

draft-gredler-idr-bgp-ls-segment-routing-ext-03—BGP Link-State extensions for Segment Routing

draft-ietf-isis-segment-routing-extensions-04—IS-IS Extensions for Segment Routing

draft-ietf-mpls-spring-lsp-ping-02—Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane

draft-ietf-ospf-segment-routing-extensions-04—OSPF Extensions for Segment Routing

draft-ietf-spring-segment-routing-15—Segment Routing Architecture

8.3.29 SONET/SDH

GR-253-CORE—SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

ITU-T Recommendation G.841—Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

8.3.30 SSH

RFC 4253—The Secure Shell (SSH) Transport Layer Protocol

draft-ietf-secsh-architecture.txt—SSH Protocol Architecture

draft-ietf-secsh-userauth.txt—SSH Authentication Protocol

draft-ietf-secsh-connection.txt—SSH Connection Protocol

draft-ietf-secsh- newmodes.txt—SSH Transport Layer Encryption Modes

draft-ietf-secsh-filexfer-13.txt—SSH File Transfer Protocol

8.3.31 Synchronization

G.781—Synchronization layer functions, 2001/09/17

G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813—Timing characteristics of SDH equipment slave clocks (SEC)

G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16

G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16

G.8261—Timing and synchronization aspects in packet networks

G.8262—Timing characteristics of synchronous Ethernet equipment slave clock

GR 1244 CORE—Clocks for the Synchronized Network: Common Generic Criteria

IEC/IEEE 61850-9-3—Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation

IEEE C37.238-2017 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, Annex E – Transport of PTP over User Datagram Protocol over Internet Protocol Version 6

ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008

ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010

ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014

ITU-T G.8275.2—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for time/phase synchronization with partial timing support from the network, issued 06/2016

RFC 5905—Network Time Protocol Version 4: Protocol and Algorithms Specification

8.3.32 TACACS+

IETF draft-grant-tacacs-02.txt—The TACACS+ Protocol

8.3.33 TLS

RFC 5246—The Transport Layer Security (TLS) Protocol Version 1.2

RFC 5922—Domain Certificates in the Session Initiation Protocol (SIP)

RFC 6460—Suite B Profile for Transport Layer Security (TLS)

RFC 8446—The Transport Layer Security (TLS) Protocol Version 1.3

8.3.34 TWAMP

RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

8.3.35 VPLS

RFC 4762—Virtual Private LAN Services Using LDP

8.3.36 VRRP

RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol

RFC 3768 Virtual Router Redundancy Protocol

RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

8.4 Proprietary MIBs

TIMETRA-ATM-MIB.mib

TIMETRA-CAPABILITY-7705-V1.mib

TIMETRA-CHASSIS-MIB.mib

TIMETRA-CLEAR-MIB.mib

TIMETRA-FILTER-MIB.mib

TIMETRA-GLOBAL-MIB.mib

TIMETRA-LAG-MIB.mib

TIMETRA-LDP-MIB.mib

TIMETRA-LOG-MIB.mib

TIMETRA-MPLS-MIB.mib

TIMETRA-OAM-TEST-MIB.mib

TIMETRA-PORT-MIB.mib

TIMETRA-PPP-MIB.mib

TIMETRA-QOS-MIB.mib

TIMETRA-ROUTE-POLICY-MIB.mib

TIMETRA-RSVP-MIB.mib

TIMETRA-SAP-MIB.mib

TIMETRA-SDP-MIB.mib

TIMETRA-SECURITY-MIB.mib

TIMETRA-SERV-MIB.mib

TIMETRA-SYSTEM-MIB.mib

TIMETRA-TC-MIB.mib

TIMETRA-VRRP-MIB.mib

Customer document and product support

Customer documentation
Customer documentation welcome page

Technical support
Product support portal

Documentation feedback
Customer documentation feedback