



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

**BASIC SYSTEM CONFIGURATION GUIDE
RELEASE 14.0.R4**

3HE 10785 AAAB TQZZA 01

Issue: 01

July 2016

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2016 Nokia. All rights reserved.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

Table of Contents

1	Getting Started.....	9
1.1	About This Guide.....	9
1.1.1	Audience.....	10
1.2	In This Chapter.....	10
1.3	Router System Configuration Process	10
2	CLI Usage	13
2.1	In This Chapter.....	13
2.2	CLI Structure	13
2.3	Navigating in the CLI	15
2.3.1	CLI Contexts.....	16
2.3.2	Basic CLI Commands.....	17
2.3.3	CLI Environment Commands	19
2.3.4	CLI Monitor Commands.....	20
2.4	Getting Help in the CLI	21
2.5	The CLI Command Prompt.....	23
2.6	Displaying Configuration Contexts	24
2.7	EXEC Files	24
2.8	CLI Script Control	25
2.9	Entering CLI Commands	25
2.9.1	Command Completion.....	26
2.9.2	Unordered and Unnamed Parameters	26
2.9.3	Editing Keystrokes.....	27
2.9.4	Absolute Paths	28
2.9.5	History	29
2.9.6	Entering Numerical Ranges.....	29
2.9.7	Pipe/Match.....	31
2.9.8	Pipe/Count.....	35
2.9.9	Redirection	36
2.10	VI Editor.....	36
2.10.1	Summary of vi Commands	37
2.10.2	Using the vi Commands	37
2.10.3	EX Commands	43
2.11	Configuration Rollback	44
2.11.1	Feature Behavior.....	45
2.11.2	Rollback and SNMP	51
2.11.3	Rescue Configuration.....	52
2.11.4	Operational Guidelines	52
2.12	Transactional Configuration.....	54
2.12.1	Basic Operation	55
2.12.2	Transactions and Rollback	57
2.12.3	Authorization.....	57
2.13	Basic CLI Command Reference	59
2.13.1	Command Hierarchies.....	59
2.13.1.1	Global Commands.....	60

2.13.1.2	Monitor Commands	60
2.13.1.3	Environment Commands	62
2.13.1.4	Candidate Commands	63
2.13.1.5	Rollback Commands	63
2.13.1.6	Management Infrastructure Control Commands	64
2.13.2	Command Descriptions	64
2.13.2.1	Global Commands	64
2.13.2.2	Monitor CLI Commands	83
2.13.2.3	CLI Environment Commands	153
2.13.2.4	Candidate Commands	157
2.13.2.5	Rollback Commands	167
2.13.2.6	Management Infrastructure Control Commands	173
2.13.2.7	Show Commands	174
3	File System Management	177
3.1	In This Chapter	177
3.2	The File System	177
3.2.1	Compact Flash Devices	178
3.2.2	URLs	178
3.2.3	Wildcards	179
3.3	File Management Tasks	181
3.3.1	Modifying File Attributes	181
3.3.2	Creating Directories	182
3.3.3	Copying Files	183
3.3.4	Moving Files	183
3.3.5	Deleting Files and Removing Directories	184
3.3.6	Displaying Directory and File Information	185
3.3.7	Repairing the File System	186
3.4	File Command Reference	187
3.4.1	Command Hierarchy	187
3.4.1.1	File Commands	187
3.4.2	Command Descriptions	187
3.4.2.1	File System Commands	187
3.4.2.2	File Commands	189
4	Boot Options	201
4.1	In This Chapter	201
4.2	System Initialization	201
4.2.1	Configuration and Image Loading	205
4.2.1.1	Persistence	207
4.2.1.2	Lawful Intercept	207
4.2.1.3	FIPS-140-2 Mode	207
4.3	Initial System Startup Process Flow	209
4.4	Configuration Notes	210
4.5	Configuring Boot Options File with CLI	211
4.6	BOF Configuration Overview	211
4.7	Basic BOF Configuration	211
4.8	Common Configuration Tasks	212
4.8.1	Searching for the BOF	213

4.8.2	Accessing the CLI.....	215
4.8.2.1	Console Connection	215
4.9	Configuring BOF Parameters	216
4.10	Service Management Tasks	216
4.10.1	System Administration Commands	216
4.10.1.1	Viewing the Current Configuration.....	217
4.10.1.2	Modifying and Saving a Configuration.....	218
4.10.1.3	Deleting BOF Parameters	219
4.10.1.4	Saving a Configuration to a Different Filename.....	219
4.10.1.5	Rebooting	220
4.11	BOF Configuration Command Reference.....	221
4.11.1	Command Hierarchies.....	221
4.11.1.1	Configuration Commands.....	221
4.11.2	Command Descriptions	222
4.11.2.1	File Management Commands	222
4.11.2.2	BOF Processing Control.....	223
4.11.2.3	Console Port Configuration	224
4.11.2.4	Image and Configuration Management	224
4.11.2.5	Management Ethernet Configuration.....	229
4.11.2.6	DNS Configuration Commands	232
4.12	BOF Show Command Reference	237
4.12.1	Command Hierarchies.....	237
4.12.2	Command Descriptions	238
4.12.2.1	BOF Show Commands.....	238
5	System Management	243
5.1	In This Chapter	243
5.2	System Management Parameters	244
5.2.1	System Information.....	245
5.2.1.1	System Name	245
5.2.1.2	System Contact	245
5.2.1.3	System Location	245
5.2.1.4	System Coordinates	246
5.2.1.5	Naming Objects	246
5.2.1.6	Common Language Location Identifier.....	246
5.2.1.7	DNS Security Extensions	247
5.2.2	System Time	247
5.2.2.1	Time Zones.....	247
5.2.2.2	Network Time Protocol (NTP).....	249
5.2.2.3	SNTP Time Synchronization	251
5.2.2.4	CRON.....	251
5.3	High Availability	252
5.3.1	HA Features	252
5.3.1.1	Redundancy	253
5.3.1.2	Nonstop Forwarding	256
5.3.1.3	Nonstop Routing (NSR).....	256
5.3.1.4	CPM Switchover	257
5.3.1.5	Synchronization	257
5.4	Synchronization and Redundancy	258

5.4.1	Active and Standby Designations	259
5.4.2	When the Active CPM Goes Offline	260
5.4.3	OOB Management Ethernet Port Redundancy	260
5.4.4	Persistence	262
5.4.4.1	Dynamic Data Persistency (DDP) Access Optimization for DHCP Leases	262
5.5	Network Synchronization	263
5.5.1	Central Synchronization Sub-System	265
5.5.2	7950 XRS-40 Extension Chassis Central Clocks	267
5.5.3	Synchronization Status Messages (SSM)	268
5.5.3.1	DS1 Signals	268
5.5.3.2	E1 Signals	268
5.5.3.3	SONET/SDH Signals	269
5.5.3.4	DS3/E3	269
5.5.4	Synchronous Ethernet	269
5.5.5	Clock Source Quality Level Definitions	270
5.5.6	IEEE 1588v2 PTP	273
5.5.6.1	PTP Clock Synchronization	280
5.5.6.2	Performance Considerations	281
5.5.6.3	PTP Capabilities	282
5.5.6.4	PTP Ordinary Slave Clock For Frequency	283
5.5.6.5	PTP Ordinary Master Clock For Frequency	284
5.5.6.6	PTP Boundary Clock for Frequency and Time	285
5.5.6.7	PTP Clock Redundancy	286
5.5.6.8	PTP Time for System Time and OAM Time	286
5.5.6.9	PTP within Routing Instances	287
5.6	System-Wide ATM Parameters	287
5.7	Link Layer Discovery Protocol (LLDP)	288
5.8	IP Hashing as an LSR	291
5.9	Ethernet Satellites	291
5.9.1	Software Repositories for Satellites	292
5.9.2	Satellite Software Upgrade Overview	293
5.9.3	Satellite Configuration	294
5.9.3.1	Satellite Client Port Association	294
5.10	Optical Extension Shelf (OES)	294
5.11	Administrative Tasks	296
5.11.1	Configuring the Chassis Mode	296
5.11.2	Saving Configurations	299
5.11.3	Specifying Post-Boot Configuration Files	299
5.11.4	Network Timing	300
5.11.5	Power Supplies	300
5.11.6	Automatic Synchronization	300
5.11.6.1	Boot-Env Option	301
5.11.6.2	Config Option	301
5.11.7	Manual Synchronization	302
5.11.7.1	Forcing a Switchover	302
5.12	System Router Instances	302
5.13	System Configuration Process Overview	303
5.14	Configuration Notes	304

5.14.1	General.....	304
5.15	Configuring System Management with CLI	305
5.16	System Management.....	306
5.16.1	Saving Configurations	306
5.17	Basic System Configuration	307
5.18	Common Configuration Tasks	307
5.18.1	System Information.....	308
5.18.1.1	System Information Parameters	309
5.18.1.2	Coordinates	310
5.18.1.3	System Time Elements.....	311
5.18.1.4	ANCP Enhancements.....	322
5.18.2	Configuring Synchronization and Redundancy	322
5.18.2.1	Configuring Persistence	322
5.18.2.2	Configuring Synchronization.....	323
5.18.2.3	Configuring Manual Synchronization.....	323
5.18.2.4	Forcing a Switchover	323
5.18.2.5	Configuring Synchronization Options	324
5.18.3	Configuring Multi-Chassis Redundancy for LAG	325
5.18.4	Configuring Mixed Mode.....	326
5.18.4.1	Enabling Mixed Mode on a 7450 System	327
5.18.5	Configuring Power Supply Parameters	328
5.18.6	Configuring ATM System Parameters	330
5.18.7	Configuring Backup Copies	330
5.18.8	Post-Boot Configuration Extension Files	332
5.18.8.1	Show Command Output and Console Messages.....	333
5.19	System Timing.....	334
5.19.1	Edit Mode	335
5.19.2	Configuring Timing References	335
5.19.3	Using the Revert Command	336
5.19.4	Other Editing Commands	336
5.19.5	Forcing a Specific Reference	337
5.20	Configuring System Monitoring Thresholds.....	338
5.20.1	Creating Events	338
5.20.2	System Alarm Contact Inputs	339
5.21	Configuring LLDP	340
5.22	System Command Reference	343
5.22.1	Command Hierarchies.....	343
5.22.1.1	Configuration Commands.....	343
5.22.1.2	System Information Commands	344
5.22.1.3	System Alarm Contact Input Commands	345
5.22.1.4	System Threshold Alarm Commands.....	345
5.22.1.5	Mixed Mode Configuration Commands	346
5.22.1.6	Persistence Commands	347
5.22.1.7	PTP Commands	348
5.22.1.8	System Time Commands	348
5.22.1.9	Cron Commands	349
5.22.1.10	Script Control Commands	350
5.22.1.11	System Synchronization Commands.....	350
5.22.1.12	System Administration (Admin) Commands.....	352

5.22.1.13	High Availability (Redundancy) Commands	352
5.22.1.14	LLDP System Commands	354
5.22.1.15	LLDP Ethernet Port Commands	354
5.22.1.16	Optical Extension Shelf (OES) Commands	355
5.22.1.17	System Router Instance Commands	355
5.22.2	System Command Reference	355
5.22.2.1	Generic Commands	355
5.22.2.2	System Information Commands	357
5.22.2.3	System Alarm Contact Input Commands	379
5.22.2.4	System Threshold Alarm Commands	382
5.22.2.5	Mixed Mode Configuration Commands	400
5.22.2.6	Persistence Commands	401
5.22.2.7	PTP Commands	405
5.22.2.8	Date and Time Commands	416
5.22.2.9	Network Time Protocol Commands	417
5.22.2.10	Cron Commands	429
5.22.2.11	Script Control Commands	434
5.22.2.12	System Synchronization Configuration Commands	438
5.22.2.13	System Administration Commands	448
5.22.2.14	Redundancy Commands	459
5.22.2.15	LLDP System Commands	480
5.22.2.16	LLDP Ethernet Port Commands	483
5.22.2.17	Optical Extension Shelf (OES) Commands	485
5.22.2.18	System Router Instance Commands	489
5.23	Show, Clear, Debug, and Tools Command Reference	491
5.23.1	Command Hierarchies	491
5.23.1.1	Show Commands	492
5.23.1.2	Clear Commands	493
5.23.1.3	Debug Commands	494
5.23.1.4	Tools Commands	494
5.23.2	Command Descriptions	495
5.23.2.1	Show Commands	495
5.23.2.2	Debug Commands	577
5.23.2.3	Tools Commands	580
5.23.2.4	Clear Commands	590
6	Standards and Protocol Support	599

1 Getting Started

1.1 About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure SR OS boot option file (BOF), file system and system management functions. Also provided are concepts and descriptions of the Command Line Interface (CLI) syntax and command usage.

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

- 7450 ESS
- 7750 SR
- 7950 XRS

[Table 1](#) lists the available chassis types for each SR OS router.

Table 1 Supported SR OS Router Chassis Types

7450 ESS	7750 SR	7950 XRS
<ul style="list-style-type: none"> • 7450 ESS-6/6v • 7450 ESS-7/12 running in standard mode (not mixed-mode) 	<ul style="list-style-type: none"> • 7450 ESS-7/12 running in mixed-mode (not standard mode) • 7750 SR-a4/a8 • 7750 SR-c4/c12 • 7750 SR-1e/2e/3e • 7750 SR-7/12 • 7750 SR-12e 	<ul style="list-style-type: none"> • 7950 XRS-16c • 7950 XRS-20/40

For a list of unsupported features by platform and chassis, refer to the *SR OS R14.0.Rx Software Release Notes*, part number 3HE10818 000x TQZZA.

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



Note: This guide generically covers Release 14.0 content and may contain some content that will be released in later maintenance loads. Please refer to the *SR OS R14.0.Rx Software Release Notes*, part number 3HE10818 000x TQZZA, for information on features supported in each load of the Release 14.0 software.

1.1.1 Audience

This guide is intended for network administrators who are responsible for configuring the 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 option, configuration, image loading, and initialization procedures
- Basic system management functions such as the system name, router location and coordinates, and CLLI code, time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), and synchronization properties

1.2 In This Chapter

This chapter provides process flow information to configure basic router and system parameters, perform operational functions with directory and file management, and boot option tasks.

1.3 Router System Configuration Process

[Table 2](#) lists the tasks necessary to configure boot option files (BOF) and system and file management functions. 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. After the hardware installation has been properly completed, proceed with the router configuration tasks in the following order:

Table 2 **Configuration Process**

Area	Task	Chapter
CLI Usage	The CLI structure	CLI Usage
	Basic CLI commands	Basic CLI Commands
	Configure environment commands	CLI Environment Commands
	Configure monitor commands	CLI Monitor Commands
Operational functions	Directory and file management	File System Management
Boot options	Configure boot option files (BOF)	Boot Options
System configuration	Configure system functions, including host name, address, domain name, and time parameters.	System Management
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support

2 CLI Usage

2.1 In This Chapter

This chapter provides information about using the command-line interface (CLI).

Topics in this chapter include:

- [CLI Structure](#)
- [Navigating in the CLI](#)
- [Basic CLI Commands](#)
- [CLI Environment Commands](#)
- [CLI Monitor Commands](#)
- [Getting Help in the CLI](#)
- [The CLI Command Prompt](#)
- [Displaying Configuration Contexts](#)
- [EXEC Files](#)
- [CLI Script Control](#)
- [Entering CLI Commands](#)
- [VI Editor](#)
- [Configuration Rollback](#)
- [Transactional Configuration](#)

2.2 CLI Structure

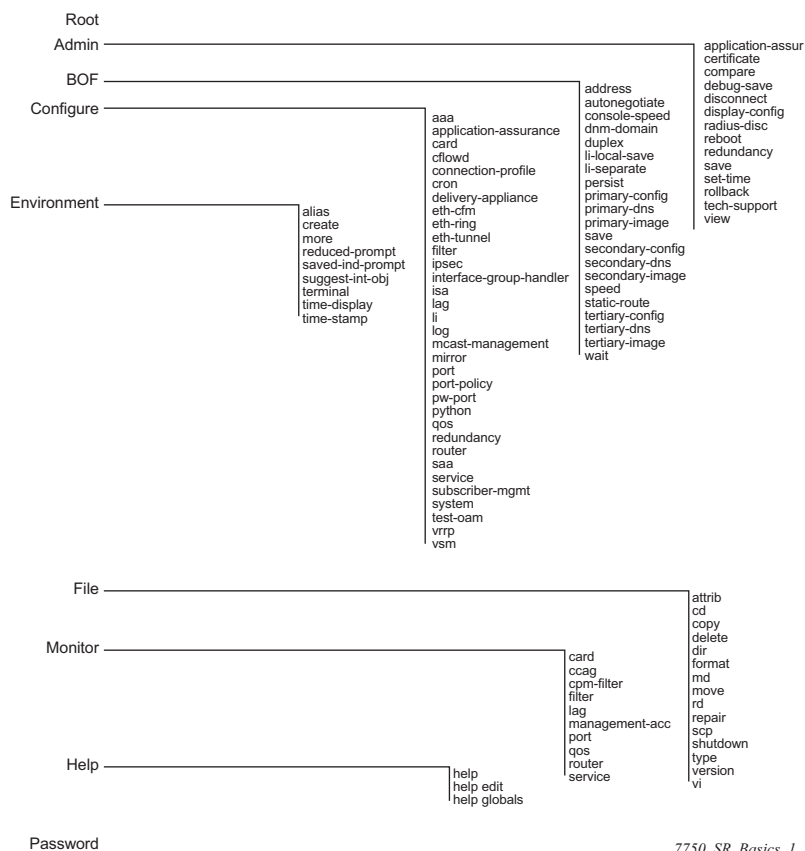
The SR OS CLI is a command-driven interface accessible through the console, Telnet and secure shell (SSH). The CLI can be used for configuration and management of routers.

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

The CLI is organized so 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.

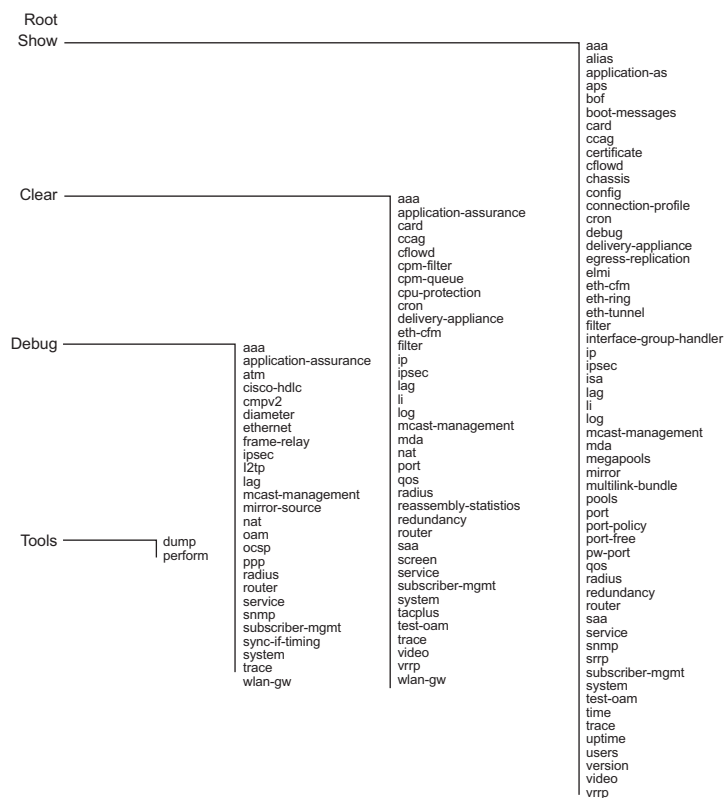
Figure 1 and Figure 2 are examples displaying the major contexts for router configuration, and are not a definitive list.

Figure 1 Root Commands



7750_SR_Basics_1

Figure 2 Operational Root Commands



7750_SR_Basics_2

2.3 Navigating in the CLI

The command outputs in the following sections are examples only; actual displays may differ depending on supported functionality and user configuration.

The following sections describe additional navigational and syntax information.

- [CLI Contexts](#)
- [Basic CLI Commands](#)
- [CLI Environment Commands](#)
- [CLI Monitor Commands](#)
- [Entering Numerical Ranges](#)

2.3.1 CLI Contexts

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

When you initially enter a CLI session, you are in the ROOT context. Navigate to another level by entering the name of successively lower contexts. For example, enter either the **configure** or **show** commands at the ROOT context to navigate to the **config** or **show** context, respectively. For example, at the command prompt (#), enter **config**. The active context displays in the command prompt.

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

In a given CLI context, enter commands at that context level by simply entering the text. It is also possible to include a command in a lower context as long as the command is formatted in the proper command and parameter syntax.

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

Method 1:

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

Method 2:

```
A:ALA-12>config# service
A:ALA-12>config>service# epipe 6
*A:ALA-12>config>service>epipe# spoke-sdp 2:6
*A:ALA-12>config>service>epipe>spoke-sdp# ingress
*A:ALA-12>config>service>epipe>spoke-sdp>ingress#
```

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

```
*A:ALA-12>config# rooter
Error: Bad command.
```


2.3.2 Basic CLI Commands

The console control commands are the commands that are used for navigating within the CLI and displaying information about the console session. Most of these commands are implemented as global commands. They can be entered at any level in the CLI hierarchy with the exception of the password command which must be entered at the ROOT level. The console control commands are listed in [Table 3](#).

Table 3 Console Control Commands

Command	Description
<Ctrl-c>	Aborts the pending command.
<Ctrl-z>	Terminates the pending command line and returns to the ROOT context.
back	Navigates the user to the parent context.
echo	Echos the text that is typed in. Primary use is to display messages to the screen within an exec file.
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.
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.
logout	Terminates the CLI session.
oam	Provides OAM test suite options. See the OAM section of the SR OS OAM and Diagnostic Guide.
password	Changes the user CLI login password. The password can only be changed at the ROOT level.
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 one second or for the specified number of seconds. Primary use is to introduce a pause within the execution of an exec file.
ssh	Opens a secure shell connection to a host.

Table 3 Console Control Commands (Continued)

Command	Description
telnet	Telnet 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.

Display the list of all system global commands by entering help globals in the CLI:

```
*A:ALA-12>config>service# help globals
back          - Go back a level in the command tree
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
info          - Display configuration for the present node
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
*A:ALA-12>config>service#
```

[Table 4](#) lists describes command syntax symbols.

Table 4 Command Syntax Symbols

Symbol	Description
	A vertical line indicates that one of the parameters within the brackets or braces is required. tcp-ack {true false}

Table 4 Command Syntax Symbols (Continued)

Symbol	Description
[]	Brackets indicate optional parameters. redirects [number seconds]
{ }	Braces indicate that one of the parameters must be selected. default-action {drop forward}
[{ }]	Braces within square brackets indicates that you must choose one of the optional parameters. <ul style="list-style-type: none">• sdp sdp-id [{gre mpls}]
Bold	Commands in bold indicate commands and keywords.
Italic	Commands in <i>italics</i> indicate that you must enter text based on the parameter. interface <i>interface-name</i>

2.3.3 CLI Environment Commands

The CLI **environment** commands are found in the **root>environment** context of the CLI tree and controls session preferences for a single CLI session. The CLI **environment** commands are listed in [Table 5](#).

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.
more	Configures whether CLI output should 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.
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.

2.3.4 CLI Monitor Commands

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

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

The <Ctrl-c> keystroke interrupts a monitoring process. Monitor command configurations cannot be saved. You must enter the command for each monitoring session. Note that if the maximum limits are configured, you can monitor the statistical information for a maximum of 60 * 999 sec ~ 1000 minutes.

The CLI monitor command contexts are listed in [Table 6](#).

Table 6 CLI Monitor Command Contexts

Command	Description
card	Enables monitoring of ingress FP queue groups.
ccag	Enables CCAG port monitoring for traffic statistics. This command is supported on the 7450 ESS and 7750 SR; additional restrictions may apply.
cpm-filter	Monitor command output for CPM filters.
filter	Enables IP and MAC filter monitoring at a configurable interval until that count is reached.
lag	Enables Link Aggregation Group (LAG) monitoring to display statistics for individual port members and the LAG.
management-access-filter	Enables management access filter monitoring.
port	Enables port traffic monitoring. The specified port(s) statistical information displays at the configured interval until the configured count is reached.
qos	Enables arbiter and scheduler statistics monitoring.
router	Enables virtual router instance monitoring at a configurable interval until that count is reached.
service	Monitors commands for a particular service.

2.4 Getting Help in the CLI

The **help** system commands and the ? key display different types of help in the CLI. [Table 7](#) lists the different help commands.

Table 7 Online Help Commands

Command	Description
help ?	List all commands in the current context.
string ?	List all commands available in the current context that start with <i>string</i> .
command ?	Displays the command's syntax and associated keywords.
command keyword ?	List the associated arguments for <i>keyword</i> in <i>command</i> .
string<Tab>	Complete a partial command name (auto-completion) or list available commands that match <i>string</i> .

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

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

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

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

```

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

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

```

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

2.5 The CLI Command Prompt

By default, the CLI command prompt indicates the device being accessed and the current CLI context. For example, the prompt: **A:ALA-1>config>router>if#** indicates the active context, the user is on the device with hostname ALA-1 in the **configure>router>interface** context. 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 the context is an existing context. A "\$" at the end of the prompt indicates the context has been newly created. New contexts are newly created for logical entities when the user first navigates into the context.

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

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

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

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

2.6 Displaying Configuration Contexts

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

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

```
*A:ALA-1>config>router# interface system
*A:ALA-1>config>router>if# info
-----
          address 10.10.0.1/32
-----
*A:ALA-1>config>router>if#

*A:ALA-1>config>router>if# info detail
-----
          address 10.10.10.103/32 broadcast host-ones
          no description
          no arp-timeout
          no allow-directed-broadcasts
          tos-marking-state trusted
          no local-proxy-arp
          no proxy-arp
          icmp
            mask-reply
            redirects 100 10
            unreachable 100 10
            ttl-expired 100 10
          exit
          no mac
          no ntp-broadcast
          no cflowd
          no shutdown
-----
*A:ALA-1>config>router>if#
```

2.7 EXEC Files

The **exec** command allows you 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 by a user 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.

2.8 CLI Script Control

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

- Where scripts are located (local compact flash, remote FTP server)
- Where to store the output of the results
- How long to keep historical script result records
- How long a script may run

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

A single script can be executing at one time. A table (SNMP `smRunTable` in the `DISMAN-SCRIPT-MIB`) is used as both an input queue of scripts waiting to be executed as well as for storage of records for completed scripts. If the input queue is full then the script request is discarded.

2.9 Entering CLI Commands

The command outputs in the following sections are examples only; actual displays may differ depending on supported functionality and user configuration.

2.9.1 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 the <Tab> key or space bar is pressed. When typing a command, the <Tab> key or space bar invokes auto-completion. If the keystrokes entered are definite, auto-completion will complete the command. If the letters are not sufficient to identify a specific command, pressing the <Tab> key or space bar will display commands matching the letters entered.

System commands are available in all CLI context levels.

2.9.2 Unordered and Unnamed Parameters

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

The following output shows different **static-route** command syntax and an example of the command usage.

```
*A:ALA-12>config>router# static-route ?
- [no] static-route {<ip-prefix/mask>|<ip-prefix> <netmask>}
[preference <preference>]
    [metric <metric>] [tag <tag>] [enable|disable] next-hop <ip-address|ip-int-name>
- [no] static-route {<ip-prefix/mask>|<ip-prefix> <netmask>}
[preference <preference>]
    [metric <metric>] [tag <tag>] [enable|disable] indirect <ip-address> [ldp
    [disallow-igp]]
- [no] static-route {<ip-prefix/mask>|<ip-prefix> <netmask>}
[preference <preference>]
    [metric <metric>] [tag <tag>] [enable|disable] black-hole
*A:ALA-12>config>router# static-route preference 1 10.1.0.0/16 metric
```

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

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

2.9.3 Editing Keystrokes

When entering a command, special keystrokes allow for editing of the command. [Table 8](#) lists the command editing keystrokes.

Table 8 Command Editing Keystrokes

Editing Action	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>
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>

2.9.4 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 path. The forward slash “/” or backward slash “\” cannot be used as an absolute path at the beginning of the command-string of the **environment alias** command. Spaces between the slash and the first command will return an error. Commands that are already global (such as ping, telnet, exit, back, etc.) cannot be executed with a forward slash “/” or backward slash “\” at the beginning of the command line.

```
*A:ALA-12# configure router
*A:ALA-12>config>router# interface system address 1.2.3.4
*A:ALA-12>config>router# /admin save
*A:ALA-12>config>router# \clear router interface
*A:ALA-12>config>router#
```

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

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

or

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

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

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

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

behaves the same as the following series of commands:

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

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

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

becomes:

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

2.9.5 History

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

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

A:ALA-42# show version
TIMOS-B-0.0.I2016 both/i386 Nokia 7450 ESS Copyright (c) 2000-2016 Nokia
All rights reserved. All use subject to applicable license agreements.
Built on Sun Oct 12 20:01:13 PDT 2008 by builder in /rel0.0/I2016/panos/main
A:ALA-42#
```

2.9.6 Entering Numerical Ranges

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

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

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

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

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

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

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

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

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

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

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

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

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. For example:

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

This will give vprn 11 the router-id “10.20.11.1”, vprn 12 the router-id “10.20.12.1”, and so on.

Specifying a range in the CLI does have limitations. These limitations are summarized in [Table 9](#).

Table 9 CLI Range Use Limitations

Limitation	Description
Up to 6 ranges (including references) may be specified in a single command, and they may not combine to more than 1000 iterations of the command.	It is possible to shut down ports 1 through 10 on XMA/MDA 1 and XMA/MDA 2: configure port 1/[1..2]/[1..10]
Ranges within quotation marks are interpreted literally.	In the CLI, 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 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, configure router interface "A[1..10]" no shutdown creates a single router interface with the name "A[1..10]". However, a command such as: configure router interface A[1..10] no shutdown creates 10 interfaces with names A1, A2 .. 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, configure port 1/1/[1..10] will attempt to change ten 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.
Command completion will cease to work when entering a range.	After entering a range in a CLI command, command and key completion, which normally occurs by pressing the <Tab> or spacebar, will cease to work. If the command line entered is correct and unambiguous, the command works properly; otherwise, an error is returned.

2.9.7 Pipe/Match

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

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

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

admin display-config | match “echo” > cf1:\test\echo_list.txt

- Task: Display all the lines that do not include “echo”:

admin display-config | match invert-match “echo”

- Task: Display the first match of “vpls” in the configuration file:

admin display-config | match max-count 1 “vpls”

- Task: Display everything in the configuration after finding the first instance of “interface”:

admin display-config | match post-lines 999999 interface

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

admin display-config | match interface | count

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

For example:

```
A:Dut-C# 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=u
p flags="
"Processing of a SDP state change event is finished and the status of all affected S
DP Bindings on SDP 101 has been updated."
```



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

A:Dut-C# admin display-config | match post-lines 5 max-
count 2 expression "OSPF.*Config"
echo "OSPFv2 Configuration"
#-----
        ospf
            timers
                spf-wait 1000 1000 1000
            exit
echo "OSPFv2 (Inst: 1) Configuration"
#-----
        ospf 1
            asbr
            router-id 1.0.0.1
            export "testall"
*A:Dut# admin display-config | match debug_mirror
        profile "debug_mirror"

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

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

*A:Dut# show log event-control | match ignore-case pre-lines 10 SyncStatus
L 2016 tmnxLogOnlyEventThrottled      MA  gen      0      0
MCPATH:
    2001 tmnxMcPathSrcGrpBlkHole       MI  gen      0      0
    2002 tmnxMcPathSrcGrpBlkHoleClear  MI  gen      0      0
    2003 tmnxMcPathAvailBwLimitReached MI  gen      0      0
    2004 tmnxMcPathAvailBwValWithinRange MI  gen      0      0
MC_REDUNDANCY:
    2001 tmnxMcRedundancyPeerStateChanged WA  gen      0      0
    2002 tmnxMcRedundancyMismatchDetected WA  gen      0      0
    2003 tmnxMcRedundancyMismatchResolved WA  gen      0      0
    2004 tmnxMcPeerSyncStatusChanged   WA  gen      0      0
```

[Table 10](#) describes regular expression symbols and interpretation (similar to what is used for route policy regexp matching). [Table 11](#) describes special characters.

Table 10 Regular Expression Symbols

String	Description
.	Matches any single character.
[]	Matches a single character that 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 that 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)
()	Define a "marked subexpression". Every matched instance will be 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 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 criteria and not a grouping delimiter.
>	Redirect output

Table 11 Special Characters

Options	Similar to	Description
[:upper:]	[A-Z]	uppercase letters
[:lower:]	[a-z]	lowercase letters
[:alpha:]	[A-Za-z]	upper- and lowercase letters

Table 11 Special Characters (Continued)

Options	Similar to	Description
\w	[A-Za-z_]	word characters
[:alnum:]	[A-Za-z0-9]	digits, upper- 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

2.9.8 Pipe/Count

The SR OS 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 in order to count the number of output lines that match a specified pattern.

For example:

```
*A:dut-c# 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:dut-c# show service service-using vprn | match Down | count
Count: 4 lines
*A:dut-c#
```

2.9.9 Redirection

The SR OS supports redirection (“>”) which allows the operator to store the output of a CLI command as a local or remote file. Redirection of output can be used to automatically store results of commands in files (both local and remote).

For example:

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

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

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

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

2.10 VI Editor

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

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

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

When opening a file, a resource check verifies that sufficient resources are available to process that file. If there are not enough resources, then the operation is denied and the operator is informed of that event.

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

2.10.1 Summary of vi Commands

The vi editor operates in two modes:

- **Command mode** — This mode causes actions to be taken on the file.
In the this mode, each character entered is a command that does something to the text file being edited; a character typed in the command mode may even cause the vi editor to enter the insert mode.
- **Insert mode** — Entered text is inserted into the file.
In the insert mode, every character typed is added to the text in the file. Hitting the Esc (Escape) key turns off the insert mode.

2.10.2 Using the vi Commands

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

- [Cutting and Pasting/Deleting Text in vi](#)
- [Inserting New Text](#)
- [Moving the Cursor Within the File](#)
- [Moving the Cursor Around the Screen](#)
- [Replacing Text](#)
- [Searching for Text or Characters](#)
- [Manipulating Character/Line Formatting](#)
- [Saving and Quitting](#)
- [Miscellaneous](#)

Table 12 Cutting and Pasting/Deleting Text in vi

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

Table 12 Cutting and Pasting/Deleting Text in vi (Continued)

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

Table 13 Inserting New Text

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

Table 14 Moving the Cursor Within the File

vi Command	Description
^B	Scroll backwards one page. A count scrolls that many pages.
^D	Scroll forwards half a window. A count scrolls that many lines.

Table 14 Moving the Cursor Within the File (Continued)

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

Table 14 Moving the Cursor Within the File (Continued)

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

Table 15 Moving the Cursor Around the Screen

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

Table 16 Replacing Text

vi Command	Description
C	Change to the end of the line from the current cursor position.

Table 16 Replacing Text (Continued)

vi Command	Description (Continued)
R	Replace characters on the screen with a set of characters entered, ending with the Escape key.
S	Change an entire line.
c	Change until cc changes the current line. A count changes that many lines.
r	Replace one character under the cursor. Specify a count to replace a number of characters.
s	Substitute one character under the cursor, and go into insert mode. Specify a count to substitute a number of characters. A dollar sign (\$) will be put at the last character to be substituted.

Table 17 Searching for Text or Characters

vi Command	Description
,	Repeat the last f, F, t or T command in the reverse direction.
/	Search the file downwards for the string specified after the /.
;	Repeat the last f, F, t or T command.
?	Search the file upwards for the string specified after the ?.
F	Search the current line backwards for the character specified after the 'F' command. If found, move the cursor to the position.
N	Repeat the last search given by / or ?, except in the reverse direction.
T	Search the current line backwards for the character specified after the T command, and move to the column after the if it's found.
f	Search the current line for the character specified after the f command. If found, move the cursor to the position.
n	Repeat last search given by / or ?.
t	Search the current line for the character specified after the t command, and move to the column before the character if it's found.

Table 18 Manipulating Character/Line Formatting

vi Command	Description
~	Switch the case of the character under the cursor.

Table 18 Manipulating Character/Line Formatting (Continued)

vi Command	Description (Continued)
<	Shift the lines up to where to the left by one shiftwidth. << shifts the current line to the left, and can be specified with a count.
>	Shift the lines up to where to the right by one shiftwidth. >> shifts the current line to the right, and can be specified with a count.
J	Join the current line with the next one. A count joins that many lines.

Table 19 Saving and Quitting

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

Table 20 Miscellaneous

vi Command	Description
^G	Show the current filename and the status.
^L	Clear and redraw the screen.
^R	Redraw the screen removing false lines.
^[Escape key. Cancels partially formed command.
^^	Go back to the last file edited.
!	Execute a shell. Not supported
&	Repeat the previous :s command.
.	Repeat the last command that modified the file.
:	Begin typing an EX editor command. The command is executed once the user types return.
@	Type the command stored in the specified buffer.
U	Restore the current line to the previous state before the cursor entered the line.
m	Mark the current position with the character specified after the 'm' command.
u	Undo the last change to the file. Typing 'u' again will re-do the change.

2.10.3 EX Commands

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

Table 21 EX commands

vi Command	Description
:ab string strings	Abbreviation. If a word is typed in vi corresponding to string1, the editor automatically inserts the corresponding words. For example, the abbreviation :ab usa United States of America would insert the words, United States of America whenever the word usa is typed in.
:map keys new_seq	Mapping. This lets you map a key or a sequence of keys to another key or a sequence of keys.
:q	Quit vi. If there have been changes made, the editor will issue a warning message.
:q!	Quit vi without saving changes.
:s/pattern/ to_pattern/ options	Substitute. This substitutes the specified pattern with the string in the to_pattern. Without options, it only substitutes the first occurrence of the pattern. If a 'g' is specified, then all occurrences are substituted.
:set [all]	Sets some customizing options to vi and EX. The :set all command gives all the possible options.
:una string	Removes the abbreviation previously defined by :ab.
:unm keys	Removes the remove mapping defined by :map.
:vi filename	Starts editing a new file. If changes have not been saved, the editor will give you a warning.
:w	Write out the current file.
:w filename	Write the buffer to the filename specified.
:w >> filename	Append the contents of the buffer to the filename.
:wq	Write the buffer and quit.

2.11 Configuration Rollback

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

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

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

The advantage of this feature are the following:

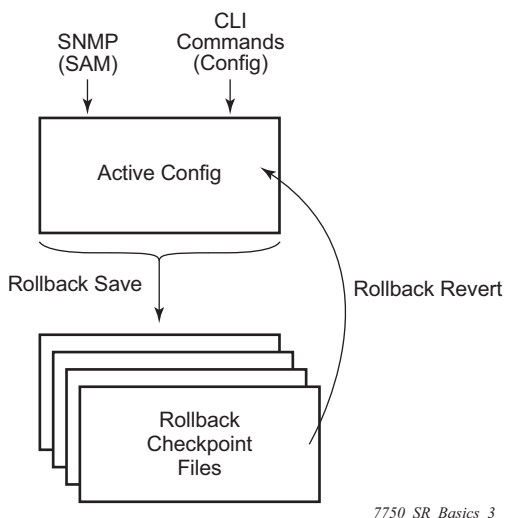
- Changes made to router configuration is performed with minimal impact on services being provided by the SR by not having to reboot the router.
- No impact in areas of configuration that did not change.

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

Configuration parameters that changed (or items that changed configuration have dependencies on) are first removed (revert to default), and the previous values are then restored (can be briefly service impacting in changed areas).

A history of changes is preserved (checkpoint ids) that allows rollback to different points, as well as examination of changes made as shown in [Figure 3](#).

Figure 3 Rollback Operation



2.11.1 Feature Behavior

The following list describes detailed behavior and CLI usage of the rollback feature:

- The user can create a rollback checkpoint, and later, revert to this checkpoint with minimal impacts to services:

```
admin>rollback# save [comment comment-string]
comment-string: an 255 char comment associated with the
checkpoint
```

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

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

...

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

- When a **rollback save** is executed, the system shifts the file suffix of all the previous checkpoints by 1 (new id = old id + 1). If there are already as many checkpoint files as the maximum number supported then the last checkpoint file is deleted.
- The maximum number of rollback checkpoints is configurable and defaults to 10 ("latest" and 1 through 9, where checkpoint file 9 is deleted during the next rollback-save).
- The location and name of the rollback checkpoint files is configurable to be local (on compact flash) or remote. The *file-url* must not contain a suffix (just a path/directory + filename). The suffix for rollback checkpoint files is .rb and is automatically appended to rollback checkpoint files.

`config>system>rollback# rollback-location file-url`

- There is no default rollback-location. If one is not specified (or it is cleared using "no rollback-location") and a rollback save is attempted, the rollback save will fail and return an error message.
- The entire set of rollback checkpoint files can be copied from the active CPM CF to the inactive CPM CF. This synchronization is done via the following command:

`admin>redundancy# rollback-sync`

- The operator can enable automatic synchronization of rollback checkpoint files between the active CPM and inactive CPM. When this automatic synchronization is enabled, a rollback save will cause the new checkpoint file to be saved to both the active and standby. The suffixes of the old checkpoint files on both active and standby CPMs are incremented.

The automatic sync only causes the new checkpoint file to be copied to both CFs (the other 9 checkpoints are not automatically copied from active to standby but that can be done manually with `admin red rollback-sync`).

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

- **config red sync {boot-env | config}** and **admin red sync {boot-env | config}** do not apply to rollback checkpoint files. These commands do not manually or automatically sync rollback checkpoint files. The dedicated `rollback-sync` commands must be used to sync rollback checkpoint files.
- Rollback files can be deleted using a dedicated rollback checkpoint deletion command.

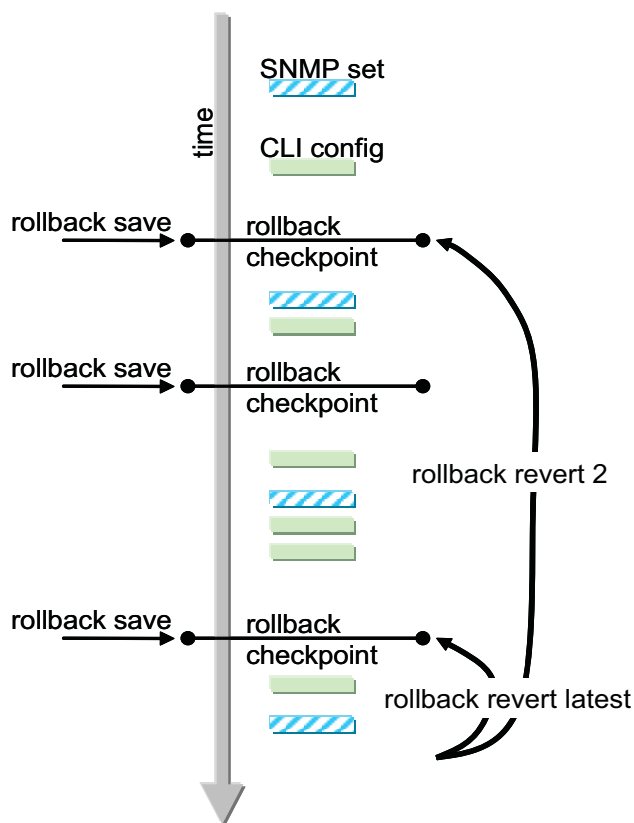
`admin>rollback# delete {latest-rb | checkpoint-id}`

- Deleting a rollback checkpoint causes the suffixes to be adjusted (decremented) for all checkpoints older than the one that was deleted (to close the "hole" in the list of checkpoint files and create room to create another checkpoint)

- If “config redundancy rollback-sync” is enabled, a rollback delete will also delete the equivalent checkpoint on the standby CF and shuffle the suffixes on the standby CF.
- If an operator manually deletes a rollback checkpoint file (using file delete) then the suffixes of the checkpoint files are NOT shuffled, nor is the equivalent checkpoint file deleted from the standby CF. This manual deletion creates a “hole” in the checkpoint file list until enough new checkpoints have been created to roll the “hole” off the end of the list.
- As shown in [Figure 4](#), support for rolling back to a previous configuration (a saved rollback checkpoint) with minimal impact on services. The previous configuration will be loaded and take operational effect:

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

Figure 4 Configuration Rollback



- A rollback revert does not affect the currently stored rollback checkpoint files (no deletions or renumbering). This means that if an operator issues the command **rollback revert 3** and then issues the **rollback-save** command, the resulting rollback checkpoint files “file-url.rb” and “file-url.rb.4” will contain the same rollback state/configuration.
- The **boot-good-exec** or **bad-exec** are not automatically executed after a rollback.
- impacts to the running services are minimized during a rollback:
 - no impact in areas of configuration that did not change
 - configuration parameters that changed (or items that changed config have dependencies on) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas). Some examples are the following:
 - If the currently active config contains **configure port 5/1/1 dwdm tdc dispersion -1000** and the rollback checkpoint contains **configure port 5/1/1 dwdm tdc dispersion -1010**, then the operational dispersion will transition from -1000, to 0 and then back to -1010 for port 5/1/1 which will cause a traffic interruption.
 - Changing the neighbor of a MC-APS port will start with neighbor 1, then be configured as no neighbor, and then will be configured with neighbor 2. Moving through the **no neighbor** intermediate state requires the working and protect circuits to be torn down and then rebuilt. This impacts the 7450 ESS and 7750 SR.
- A Rollback will undo any SNMP sets or direct CLI config commands that occurred since the last checkpoint creation.
- During the period when a node is processing a rollback revert, both CLI commands (from other users) and SNMP commands will continue to be processed. The only commands that are blocked during a rollback revert are other rollback commands including **revert**, **save**, and **compare** (only one **rollback** command can be executing at a time in one node).
- Commands are available to view and compare the various rollback checkpoints to current operating and candidate configurations.
- Rollback checkpoint files are not guaranteed to be in any particular format. They are not interchangeable with normal config files or exec scripts. A normal config file (from an admin save) cannot be renamed as a rollback checkpoint and then referenced for a rollback revert operation. Only rollback checkpoint files generated with rollback save can be used to rollback revert.
- If a hardware change is made after a rollback-save then:
 - a rollback can be executed as long as the hardware change was an addition of hardware to the node (for example, added a new card or IOM into a previously empty slot).

- a rollback is not guaranteed to work if hardware was removed or changed (for example, XCM/IOM was removed, or XMA/MDA was swapped for a different XMA/MDA type).
- Rollback across a change to the following parameters is not supported:
 - chassis-mode
 - mixed-mode
 - the SR | SS capability of a card (**configure card capability sr | ess**)
 - configure isa application-assurance-group minimum-isa-generation
- Rollback is supported even after an **admin reboot** is performed (or changes the primary config in the bof is changed and an **admin reboot** is performed). **Admin reboot** does not “break the chain” for rollback.
- Lawful Intercept configuration under the **config>li** branch is not affected by a rollback or rescue. LI configuration is not saved in the rollback checkpoint or rescue file, and a rollback revert does not touch any config under the **config>li** branch.
- Any configuration or state change performed under the debug branch of CLI is not saved in the rollback checkpoint file nor impacted by a rollback.
- Rollbacks to a checkpoint created in a more recent release is not supported (for example, node running in 9.0r5 cannot rollback to a checkpoint created in 9.0r7).
- The following list captures some side effects and specific behaviors of a Rollback revert. Some of these side effects are not related purely to configuration (that is, in the CLI config branch) and may have interactions with tools commands, RADIUS, etc.
 - SAA jobs that are running when a rollback revert is initiated, and need configuration changes due to the rollback, will be stopped. If the SAA job is a continuous type then it will be re-started as part of the rollback revert after the config changes have been applied (just as if the operator had typed “no shutdown” for the continuous SAA job). Non-continuous SAA jobs that were modified by the rollback would need to be manually restarted if they need to be run again.
 - If **max-nbr-mac-addr** is reduced as part of the revert and the number of mac addresses in the forwarding database is greater than the max-nbr-mac-addr, then the rollback is aborted (before any actions are taken) and an informative error message is provided. The operator must take actions to remove the mac addresses if they wish to proceed with the rollback.
 - If active subscribers and/or subscriber hosts and/or DHCP lease state are present then some associated configuration changes may be blocked (just as those same changes would be blocked if an operator tried to make them via CLI – trying to delete an sla-profile being used by active subscriber hosts, or trying to change a nat-policy in a sub-profile). If certain configuration changes associated with the hosts or lease states are

required as part of the rollback but those changes are blocked, then for each blocked configuration item a warning will be printed, that particular configuration item will not be changed and the rollback will continue. This is supported on the 7450 ESS and 7750 SR.

- After multi-chassis peer shutdown or configuration changes that affect the contents of the distributed database (for example, sync tag creation or deletion), further configuration changes related to that peer may be temporarily refused. The duration of the temporary configuration freeze will depend on the size of the distributed database. A rollback attempting to make those refused configuration changes will fail and an error message will be provided to the CLI user.
- If a **force-switchover** command (for example, **tools perform service id 1 endpoint "x" force-switchover spoke-sdp-fec 1**) has been applied to a spoke-sdp-fec of a dynamic multi-segment pseudo wire, and a rollback revert needs to change the admin state of the spoke-sdp-fec (for example, to modify spoke-sdp-fec parameters that may be dependent on admin state), then the rollback revert will automatically remove the force-switchover and the node will revert to whatever is the best spoke-sdp in the redundant set.
- Rollback impacts the configuration state of the router, and as with normal operator CLI or SNMP configuration changes, additional actions or steps may need to occur before certain configuration changes take operational effect. Some examples include:
 - Configuration changes that require a **shutdown** and then **no-shutdown** to be done by an operator in order to take operational effect also need this manual shut/no-shut to be performed by the operator in order to take operational effect after a rollback if the rollback changes those configuration items. Some examples include:
 - Changes to Autonomous System or Confederation value require a BGP shut/no-shut.
 - Changes to VPRN Max-routes requires a shut/no-shut on the VPRN service.
 - Changes to OSPF/ISIS export-limit require a shut/no-shut on OSPF/ISIS.
 - Configuration changes to an msap-policy that normally requires a **tools perform subscriber-mgmt eval-msap** command to take operational effect on subscribers that are already active. Rollback will change the msap-policy configuration, but if it is required to have the configuration changes applied to the active subscribers then the operator will have to run the eval-msap tools command.
- Any uncommitted changes (that is, the **begin** command was entered, some changes made, but the **commit** command was never entered) in the following areas will be lost/cleared when a rollback revert is initiated:

- **config>app-assure>group policy**
- **config>router>policy-options**
- **config>system>sync-if-timing**
- Some **card** and **mda** commands require a reboot, remove or rebuild of an entire card or XMA/MDA. When these commands need to be executed as part of a rollback, the impacted cards/mdas will be listed in a warning and the operator will be prompted with a single y/n prompt to decide whether to proceed or not. This prompting will not occur for a rollback initiated via SNMP, nor if the operator uses the **now** keyword with the rollback revert command. Some examples of card and mda commands that may cause a prompt are:
 - **configure>card>card-type**
 - **configure>card>named-pool-mode (7450 ESS and 7750 SR)**
 - **configure>card>mda**
 - **configure>card>mda>mda-type**
- Although the use of the Control-C key combination is not recommended during a rollback revert, it is supported (via CLI or SNMP). Interrupting a rollback revert may leave the router in a state that is not necessarily something between the old active config and the rollback checkpoint since the rollback processing may have been in the middle of tearing things down or rebuilding configurations. A strong warning is issued in this case to indicate that the operator must examine the config and potentially issue another rollback revert to return to a known (and coherent) configuration.
- An HA CPM switchover during a rollback revert will cause the rollback operation to abort. The newly active CPM will have an indeterminate configuration. When an HA switchover occurs during a rollback (or within a few seconds of a rollback completing), the operator is advised to repeat the rollback revert operation to the same checkpoint.
- A rollback revert operation does not check authorization of each command that is applied during the revert. Permission to execute the revert operation (authorization for the “admin rollback revert” command itself) should only be given to users who are allowed to initiate a rollback revert. It is generally advised to only allow system administrators access to the file system where the rollback files are stored so that they cannot be manually edited.

2.11.2 Rollback and SNMP

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

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

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

2.11.3 Rescue Configuration

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

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

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

2.11.4 Operational Guidelines

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

- Both **admin save** and **rollback save** should be performed periodically:
- Use **admin save** to backup a complete configuration file that can be used during router reboot.
 - Used with a reboot as a last resort.
 - Do an admin save after any major h/w changes or major service changes.
 - Should be performed after any software upgrade.
- Use **rollback-save** to create a rollback checkpoint.
 - Used for intermediate checkpoints that can be recovered with minimal impacts to services.
 - Should be performed each time that a moderate amount configuration changes have been made.
 - Should be performed after any h/w changes.
 - Should be performed after any s/w upgrade.

- Could also be scheduled with cron (for example, once every 1 or 2 weeks).
- A new **rescue-save** must be created when hardware is changed.
- Rollback-checkpoint files are not editable nor compatible/interchangeable with config files (generated with **admin save**).
- Do not continue to repeat the **rollback save**, **rollback save**, **rollback save** over the course of weeks/months without also doing executing an occasional **admin save**. In a serious situation, use one of the saved configs to use as the primary config for an **admin reboot**.
- Software Upgrade: It is recommended to create a Rollback Checkpoint (**admin rollback save**), in addition to saving the configuration (**admin save**), after an upgrade has been performed and the system is operating as expected. This will ensure a good checkpoint fully compatible with the new release is available at a point shortly after the upgrade.
- An operator could create a set of rollback checkpoints to support busy/quiet days or weekend/weekday and use cron to shift between them.
- It is beneficial to create a rollback checkpoint before a rollback revert is initiated (especially if there have been significant config changes since the last checkpoint was created). If the rollback is especially significant (a lot of major changes) it is also a good practice to do perform an **admin save** in case a full reboot is required to recover from an issue.
- A rollback failure may occur in some limited cases where the node needs a long time to complete one of the resulting configuration changes. Some examples include X and Y. If a rollback (for example, rollback revert 5) fails during execution, it should be attempted again. The second attempt will typically complete the remaining configuration changes required to fully revert to the desired checkpoint.
- When a new backup CPM is commissioned, the user execute the **admin redundancy rollback-sync** command to copy the entire set of rollback files from the active CPM cf to the new standby CPM cf. If the operator wants the system to automatically copy new rollback checkpoints to both cfs whenever a new checkpoint is created, then the **config redundancy rollback-sync** should be configured.
- An HA CPM switchover during a rollback revert will cause the rollback operation to abort. The newly active CPM will have an indeterminate configuration. A log event is created in this case to warn the operator. When an HA switchover occurs during a rollback (or within a few seconds of a rollback completing), the operator is advised to repeat the rollback revert operation to the same checkpoint.

- A rollback checkpoint stores the rollback-location and the local/remote-max-checkpoint values, and as such a rollback revert operation can change those values. If an operator changes the local/remote-max-checkpoint values it is recommended to delete all the existing checkpoints (otherwise a subsequent rollback revert could change the max back to a previous value).
- If a warning prompt (**y/n**) is displayed when a rollback revert is initiated, it is highly suggested to respond **no** to the warning prompt the first time, save a rollback checkpoint before attempting this rollback revert, and then executing the revert again and responding **yes**. If the rollback encounters problems then a revert to the saved checkpoint can be used to go back to the initial configuration state.

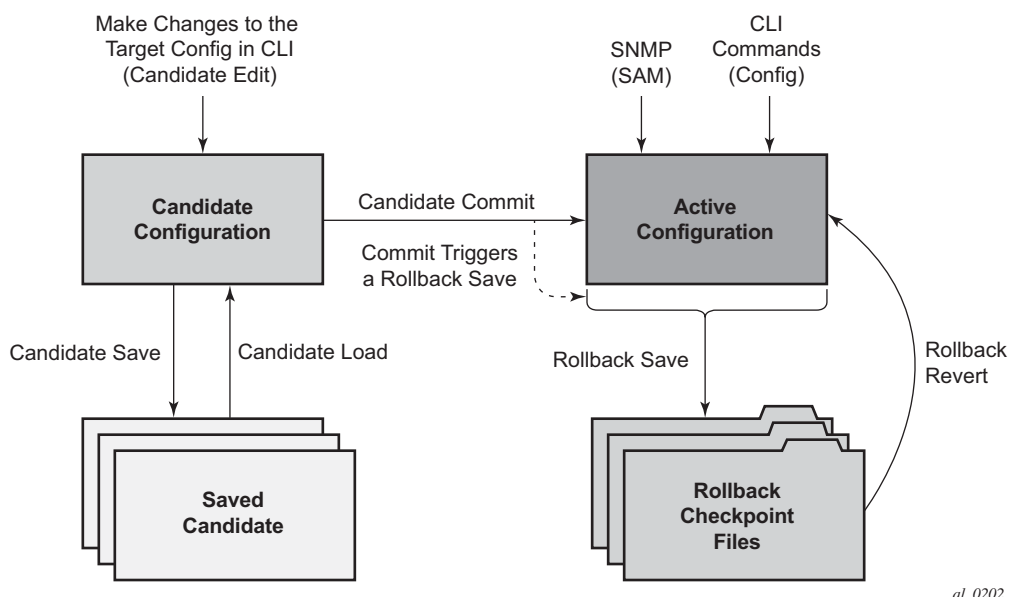
2.12 Transactional Configuration

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

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

Transactional Configuration and Configuration Rollback support combine to provide the operational model depicted in [Figure 5](#).

Figure 5 Router Configuration with Rollback and Transactions



al_0202

2.12.1 Basic Operation

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

In edit-cfg mode the operator builds a set candidate configuration changes using the same CLI tree as 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 in the SR OS, there is also a single global candidate configuration instance. All users make changes in the same global candidate configuration and a commit operation by any user will commit the changes made by all users.

Users have the ability to exclusively create a candidate configuration by blocking other users (and sessions of the same user) from entering edit-cfg mode.

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

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 candidate editing commands (**copy**, **insert**, etc) are available to correct and reorder the candidate configuration.

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

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

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

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

Failure of a commit may be due to one or more of several reasons including:

- **Misordering:** The candidate configuration has changes that are not in the correct order (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 configuration and options that are not valid and are rejected when the SR OS attempts to have them take operational effect.

- Out of resources: The application of the candidate may exhaust various system resources (queues, for example).

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

Standard line-by-line (immediate operational effect upon pushing the enter/return key) non-transactional CLI and SNMP commands are not blocked during the creation/editing of a candidate or the processing of a commit. These commands take immediate effect as normal.

2.12.2 Transactions and Rollback

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

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

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

2.12.3 Authorization

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

The candidate **load** and **save** operations (if the operator's profile allows access to the candidate load and save commands) will load and save only those items that the user is authorized to access.

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

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

The candidate **commit** and **discard** operations (along with **rollback revert**) operate on the entire candidate and impact all items (authorization does not apply).

2.13 Basic CLI Command Reference

2.13.1 Command Hierarchies

- [Global Commands](#)
- [Monitor Commands](#)
- [Environment Commands](#)
- [Candidate Commands](#)
- [Rollback Commands](#)
- [Management Infrastructure Control Commands](#)

2.13.1.1 Global Commands

- **back**
- **echo** [*text-to-echo*] [*extra-text-to-echo*] [*more-text*]
- **enable-admin**
- **exec** [-echo] [-syntax] *filename*
- **exit** [all]
- **help**
- **history**
- **info** [detail] [objective]
- **logout**
- **mrinfo** [*ip-address* | *dns-name*] [**router** *router-instance*]
- **mstat source** [*ip-address* | *dns-name*] [**group** *grp-ip-address*] [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-instance*] [**wait-time** *wait-time*]
- **mtrace source** [*ip-address* | *dns-name*] [**group** *grp-ip-address*] [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-instance*] [**wait-time** *wait-time*]
- **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** [*ip-addr* | *dns-name* | *username@ip-addr*] [-l *username*] [-v *SSH-version*] [**router** *router-instance*] [**service-name** *service-name*]
- **telnet** [*ip-address* | *dns-name*] [*port*] [**router** *router-instance*]
- **traceroute** [*ip-address* | *dns-name*] [**ttl** *value*] [**wait** *milliseconds*] [**no-dns**] [**source** *ip-address*] [**tos** *type-of-service*]
- **tree** [detail] [flat] [*command-string*]
- **write** {*user* | **broadcast**} *message-string*

2.13.1.2 Monitor Commands

monitor

- **card** *slot-number* **fp** *ip-numbering* **ingress** {**access** | **network**} **queue-group** *queue-group-name* **instance** *instance-id* [**interval** *seconds*] [**repeat** *repeat*] [**policer** *policer-id*] [**absolute** | **percent-rate** | *reference-rate*]
- **ccag** *ccag-id* [**path** {**a** | **b**}] [**type** {**sap-sap** | **sap-net** | **net-sap**}] [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
- **cpm-filter**
 - **ip** **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
 - **ipv6** **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
 - **mac** **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
- **filter**
 - **ip** *ip-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
 - **ipv6** *ipv6-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
 - **mac** *mac-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
- **lag** *lag-id* [*lag-id...*(up to 5 max)] [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
- **management-access-filter**
 - **ip** **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

- **ipv6** entry *entry-id* [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
- **mac** entry *entry-id* [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
- **port** *port-id* [*port-id...*(up to 5 max)] [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
[*multiclass*]
- **port** all-ethernet-rates [*interval seconds*] [*repeat repeat*]
- **port** atm [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
- **qos**
 - **arbiter-stats**
 - **card** *slot-number* **fp** *fp-number* **queue-group** *queue-group-name* **instance**
instance-id [*ingress*] [*access* | *networks*] [*interval seconds*] [*repeat*
repeat] [*absolute* | *percent-rate* | *reference-rate*] [*arbiter root* | *name*]
 - **customer** *customer-id* **site** *customer-site-name* [*arbiter root* | *name*] [*ingress*
| *egress*] [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **port** *port-id* **egress** *network* **queue-group** *queue-group-name* **instance**
instance-id [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*] [*arbiter root*
| *name*]
 - **sap** *sap-id* [*arbiter name* | *root*] [*ingress* | *egress*] [*interval seconds*] [*repeat*
repeat] [*absolute* | *rate*]
 - **subscriber** *sub-ident-string* [*arbiter name* | *root*] [*ingress* | *egress*] [*interval*
seconds] [*repeat repeat*] [*absolute* | *rate*]
 - **port** *port-id* **exp-secondary-shaper** *shaper-name* [*interval seconds*] [*repeat repeat*]
[*absolute* | *rate*]
 - **port** *port-id* **vport** *name* **monitor-threshold** [*interval seconds*] [*repeat repeat*]
 - **scheduler-stats**
 - **customer** *customer-id* **site** *customer-site-name* [*scheduler scheduler-name*]
[*ingress* | *egress*] [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **port** *port-id* **queue-group** *queue-group-name* [*ingress* | *egress*] [*interval*
seconds] [*repeat repeat*] [*absolute* | *rate*] [*access* | *network*] [*instance*
instance-id]
 - **port** *port-id* **vport** *name* [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **sap** *sap-id* [*scheduler scheduler-name*] [*ingress* | *egress*] [*interval seconds*]
[*repeat repeat*] [*absolute* | *rate*]
 - **sap** *sap-id* **encap-group** *group-name* [*member encap-id*] [*scheduler*
scheduler-name] [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **subscriber** *sub-ident-string* [*scheduler scheduler-name*] [*ingress* | *egress*]
[*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **subscriber** *sub-ident-string* [*interval seconds*] [*repeat repeat*] [*absolute* |
rate] **sap** *sap-id* **sla-profile** *sla-profile-name*
- **router** [*router-instance*]
 - **bgp**
 - **neighbor** *ip-address* [*ip-address...*(up to 5 max)] [*interval seconds*] [*repeat*
repeat] [*absolute* | *rate*]
 - **isis**
 - **statistics** [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **ldp**
 - **session** *ldp-id* [*ldp-id...*(up to 5 max)] [*interval seconds*] [*repeat repeat*]
[*absolute* | *rate*]
 - **statistics** [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **mpls**
 - **interface** *interface* [*interface...*(up to 5 max)] [*interval seconds*] [*repeat repeat*]
[*absolute* | *rate*]
 - **lsp-egress-stats** *lsp-name* [*interval seconds*] [*repeat repeat*] [*absolute* | *rate*]
 - **lsp-ingress-stats** **lsp** *lsp-name* [*interval seconds*] [*repeat repeat*] [*absolute* |
rate]

- **ospf** [*ospf-instance*][
 - **interface** *interface* [*interface...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **neighbor** *ip-address* [*ip-address...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **virtual-link** *nbr-rtr-id* *area* *area-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **virtual-neighbor** *nbr-rtr-id* *area* *area-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **ospf3**
 - **interface** *interface* [*interface...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **neighbor** *ip-address* [*ip-address...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **neighbor** [*router-id*] [*interface-name*] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **virtual-link** *nbr-rtr-id* *area* *area-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **virtual-neighbor** *nbr-rtr-id* *area* *area-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **pim**
 - **group** *grp-ip-address* [*source ip-address*] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **rip**
 - **neighbor** *neighbor* [*neighbor...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **rsvp**
 - **interface** *interface* [*interface...*(up to 5 max)] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **vrrp**
 - **instance** *interface* *interface-name* *vr-id* *virtual-router-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
- **service**
 - **id** *service-id*
 - **sap** *sap-id* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **sdp** *sdp-id* [*far-end*] *ip-address* [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]
 - **subscriber** *sub-ident-string* **sap** *sap-id* **sla-profile** *sla-profile-name* [*base* | *ingress-queue-id* *ingress-queue-id* | *egress-queue-id* *egress-queue-id*] [*interval seconds*] [**repeat** *repeat*] [*absolute* | *rate*]

2.13.1.3 Environment Commands

- <root>
 - **environment**
 - **alias** *alias-name* *alias-command-name*
 - **no alias** *alias-name*
 - **[no] create**
 - **[no] more**
 - **reduced-prompt** [*no. of nodes in prompt*]
 - **no reduced-prompt**
 - **[no] saved-ind-prompt**

- **suggest-internal-objects**
- [no] **terminal**
 - **length** *lines*
 - **width** *width*
- **time-display** {*local* | *utc*}

2.13.1.4 Candidate Commands

```
<root>
  — 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]
  — info operational operational

show
  — system
    — candidate
```

2.13.1.5 Rollback Commands

```
<root>
  — admin
    — rollback
      — compare [to source2]
      — compare source1 to source2
      — delete {latest-rb | checkpoint-id | rescue}
      — revert {latest-rb | checkpoint-id | rescue} [now]
      — save [comment comment-string] [rescue]
      — view [latest-rb | checkpoint-id | rescue]
    — view {active-cfg | rescue | latest-rb | checkpoint-id}

config
  — system
    — rollback
```

- [no] **rollback-location** *file-url rollback filename*
- [no] **rescue-location** *file-url*
- [no] **local-max-checkpoints** *local-max-checkpoints*
- [no] **remote-max-checkpoints** *local-remote-checkpoints*

2.13.1.6 Management Infrastructure Control Commands

```
config
  — system
    — management {cli}
      — configuration
        — immediate
```

2.13.2 Command Descriptions

2.13.2.1 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 ospf context, the back command moves the cursor to the config router context level.
Default	N/A

echo

Syntax	echo [<i>text-to-echo</i>] [<i>extra-text-to-echo</i>] [<i>more-text</i>]
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.
Default	N/A
Parameters	<i>text-to-echo</i> — 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	<global>
Description	See the description for the admin-password command. If the admin-password is configured in the config>system>security>password context, then any user can enter a special administrative mode by entering the enable-admin command.

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

Once the **enable-admin** command is entered, the user is prompted for a password. If the password matches, the user is given 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 shows a password configuration example:

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

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

- show users — administrator can know which users are in this mode
- Enter the **enable-admin** command again at the root prompt and an error message will be returned.

```
A:ALA-1# show users
=====
User Type From Login time Idle time
=====
admin Console -- 10AUG2006 13:55:24 0d 19:42:22
admin Telnet 10.20.30.93 09AUG2004 08:35:23 0d 00:00:00 A
-----
Number of users : 2
'A' indicates user is in admin mode
=====
A:ALA-1#
```

```
A:ALA-1# enable-admin
MINOR: CLI Already in admin mode.
A:ALA-1#
```

Default N/A

exec

Syntax **exec** [-echo] [-syntax] {filename | <<[eof_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:

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

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

Default N/A

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 will be able to find invalid commands and keywords, but it will not be able to validate erroneous user-supplied parameters.

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 will be silently ignored. The **exec** command will indicate the command error line number when the stdin input is terminated with an end-of-file input.

eof_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	<p>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.</p> <pre>A:ALA-1# configure A:ALA-1>config# router A:ALA-1>config>router# ospf A:ALA-1>config>router>ospf# exit A:ALA-1>config>router# exit A:ALA-1>config# exit</pre> <p>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.</p> <pre>A:ALA-1# configure router ospf A:ALA-1>config>router>ospf# exit A:ALA-1#</pre> <p>The exit all command moves the cursor all the way back to the root level.</p> <pre>A:ALA-1# configure A:ALA-1>config# router A:ALA-1>config>router# ospf A:ALA-1>config>router>ospf# exit all A:ALA-1#</pre>
Default	N/A
Parameters	all — exits back to the root CLI context

help

Syntax	help help edit help global help special-characters
Context	<global>
Description	<p>This command provides a brief description of the help system. The following information is shown:</p> <pre>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.</pre>

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.

Default N/A

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 global — displays help on global commands

Available global commands:

```
back          - Go back a level in the command tree
echo          - Echo the text that is typed in
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
info         - Display configuration for the present node
logout       - Log off this system
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 ? — display command's 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	<p>This command lists the last 30 commands entered in this session.</p> <p>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.</p>

Example:

```
A:ALA-1# history
68 info
69 exit
70 info
71 filter
72 exit all
73 configure
74 router
75 info
76 interface "test"
77 exit
78 reduced-prompt
79 info
80 interface "test"
81 icmp unreachable exit all
82 exit all
83 reduced-prompt
84 configure router
85 interface
86 info
87 interface "test"
88 info
89 reduced-prompt
90 exit all
91 configure
92 card 1
93 card-type
94 exit
95 router
96 exit
97 history
```

```
A:ALA-1# !91
A:ALA-1# configure
A:ALA-1>config#
```

Default N/A

info

Syntax `info [detail] [objective]`

Context <global>

Description This command displays the running configuration for the configuration context.

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

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 “include-dynamic” **objective** keyword includes configuration parameters from dynamic sources such as VSD or dynamic data service Python scripts. These dynamic configuration parameters are not saved in the configuration file.

Example:

```
A:ALA-48>config>router>mpls# info
-----
admin-group "green" 15
admin-group "red" 25
admin-group "yellow" 20
interface "system"
exit
interface "to-104"
  admin-group "green"
  admin-group "red"
  admin-group "yellow"
  label-map 35
    swap 36 nexthop 10.10.10.91
    no shutdown
  exit
exit
path "secondary-path"
  hop 1 10.10.0.111 strict
  hop 2 10.10.0.222 strict
  hop 3 10.10.0.123 strict
  no shutdown
exit
path "to-NYC"
  hop 1 10.10.10.104 strict
  hop 2 10.10.0.210 strict
  no shutdown
exit
path "to-104"
```

```
        no shutdown
    exit
    lsp "to-104"
        to 10.10.10.104
        from 10.10.10.103
        rsvp-resv-style ff
        cspf
...
-----
A:ALA-48>config>router>mpls#
A:ALA-48>config>router>mpls# info detail
-----
    frr-object
    no resignal-timer
    admin-group "green" 15
    admin-group "red" 25
    admin-group "yellow" 20
    interface "system"
        no admin-group
        no shutdown
    exit
    interface "to-104"
        admin-group "green"
        admin-group "red"
        admin-group "yellow"
        label-map 35
            swap 36 nexthop 10.10.10.91
        no shutdown
    exit
    no shutdown
    exit
    path "secondary-path"
        hop 1 10.10.0.111 strict
        hop 2 10.10.0.222 strict
        hop 3 10.10.0.123 strict
        no shutdown
    exit
    path "to-NYC"
        hop 1 10.10.10.104 strict
        hop 2 10.10.0.210 strict
        no shutdown
    exit
    path "to-104"
        no shutdown
    exit
    lsp "to-104"
        to 10.10.10.104
        from 10.10.10.103
        rsvp-resv-style ff
        adaptive
        cspf
        include "red"
        exclude "green"
        adspec
        fast-reroute one-to-one
            no bandwidth
            no hop-limit
            node-protect
    exit
```

```
hop-limit 10
retry-limit 0
retry-timer 30
secondary "secondary-path"
    no standby
    no hop-limit
    adaptive
    no include
    no exclude
    record
    record-label
    bandwidth 50000
    no shutdown
exit
primary "to-NYC"
    hop-limit 50
    adaptive
    no include
    no exclude
    record
    record-label
    no bandwidth
    no shutdown
exit
no shutdown
exit
...
-----
A:ALA-48>config>router>mpls#
```

Default	N/A
Parameters	<p>detail — displays all configuration parameters including parameters at their default values</p> <p>objective — provides an output objective that controls the configuration parameters to be displayed</p> <p>Values <i>include-dynamic</i> — includes configuration parameters from dynamic sources such as vsd or dynamic data service Python scripts</p>

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 re-created.

Default N/A

mrinfo

Syntax **mrinfo** [*ip-address* | *dns-name*] [**router** *router-instance*]

Context <global>

Description This command is used to print relevant multicast information from the target multicast router. Information displayed includes adjacency information, protocol, metrics, thresholds, and flags from the target multicast route.

Default N/A

Parameters *ip-address* — specifies the ip-address of the multicast capable target router
dns-name — specifies the DNS name (if DNS name resolution is configured)

Values 63 characters maximum

router *router-instance* — specifies the router name or service ID

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

Default Base

mstat

Syntax **mstat source** [*ip-address* | *dns-name*] [**group** *grp-ip-address*] [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-instance*] [**wait-time** *wait-time*]

Context <global>

Description This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information.

Default N/A

Parameters *ip-address* — specifies the ip-address of the multicast capable target router
dns-name — specifies the DNS name (if DNS name resolution is configured)

Values 63 characters maximum

group *group-ip-address* — specifies the multicast address of the group to be displayed

destination *dst-ip-address* — specifies the unicast destination address

hop count — specifies the maximum number of hops that will be traced from the receiver back toward the source

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router *router-instance* — specifies the router name or service ID

Values

<i>router-name:</i>	Base, management
<i>service-id:</i>	1 to 2147483647

Default Base

wait-time *wait-time* — specifies the number of seconds to wait for the response

Values 1 to 60

mtrace

Syntax **mtrace source** [*ip-address* | *dns-name*] [**group** *grp-ip-address*] [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-instance*] [**wait-time** *wait-time*]

Context <global>

Description This command traces a multicast path from a source to a receiver.

Default N/A

Parameters

ip-address — specifies the ip-address of the multicast capable target router

dns-name — specifies the DNS name (if DNS name resolution is configured)

Values 63 characters maximum

group *group-ip-address* — specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) will be used. This will suffice if packet loss statistics for a particular multicast group are not needed.

destination *dst-p-address* — specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response will also be returned to the address specified as the receiver.

hop *hop* — specifies the maximum number of hops that will be traced from the receiver back toward the source.

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — specifies the router name or service ID

Values

<i>router-name:</i>	Base, management
<i>service-id:</i>	1 to 2147483647

Default Base

wait-time *wait-time* — specifies the number of seconds to wait for the response

Values 1 to 60

password

Syntax	password
Context	<root>
Description	<p>This command changes a user's CLI login password.</p> <p>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.</p> <p>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.</p> <p>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 to access the CLI.</p> <p>A user cannot configure a non-conformant password for themselves using the global password command. A password value that does not conform to the minimum-length or other password complexity rules can be configured using the config>system>security>user>password command (for example, by an administrator), but a warning is provided in the CLI. This allows, for example, an administrator to configure a non-conformant password for a user.</p>
Default	N/A

ping

Syntax	ping { <i>ip-address</i> <i>ipv6-address</i> <i>dns-name</i> } [rapid detail] [ttl <i>time-to-live</i>] [tos <i>type-of-service</i>] [size <i>bytes</i>] [pattern <i>pattern</i>] [source <i>ip-address</i>] [interval <i>seconds</i>] [{ next-hop <i>ip-address</i> } { interface <i>interface-name</i> } bypass-routing] [count <i>requests</i>] [do-not-fragment] [router <i>router-instance</i>] [timeout <i>timeout</i>]
Context	<global>
Description	This command is the TCP/IP utility that is used to verify IP reachability.

Default	N/A
Parameters	<p><i>ip-address</i> / <i>dns-name</i> — the remote host to ping. The IP address or the DNS name (if DNS name resolution is configured) can be specified.</p> <p><i>ipv6-address</i> — the IPv6 IP address (applies to the 7750 SR and 7950 XRS)</p> <p>Values <i>x</i>: <i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i> (eight 16-bit pieces) <i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>d</i>.<i>d</i>.<i>d</i>.<i>d</i> <i>x</i>: 0 to FFFF H <i>d</i>: 0 to 255 D</p> <p>rapid detail — 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.</p> <p>The detail parameter includes in the output the interface on which the ping reply was received.</p> <p>Example output:</p> <pre> A:ALA-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 A:ALA-1# </pre> <p>ttl <i>time-to-live</i> — the IP Time To Live (TTL) value to include in the ping request, expressed as a decimal integer</p> <p>Values 0 to 128</p> <p>tos <i>type-of-service</i> — the type-of-service (TOS) bits in the IP header of the ping packets, expressed as a decimal integer</p> <p>Values 0 to 255</p> <p>size <i>bytes</i> — the size in bytes of the ping request packets</p> <p>Values 0 to 65507</p> <p>Default 56 bytes (actually 64 bytes because 8 bytes of ICMP header data are added to the packet)</p> <p>pattern <i>pattern</i> — a 16-bit pattern string to include in the ping packet, expressed as a decimal integer</p> <p>Values 0 to 65535</p>

source *ip-address* — the source IP address to use in the ping requests, in dotted decimal notation

Values 0.0.0.0 to 255.255.255.255

Default the IP address of the egress IP interface

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

Values 1 to 10000

Default 1

next-hop *ip-address* — disregards the routing table and will send 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

interface *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.

count *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 (does not apply to ICMPv6).

router *router-instance* — specifies the router name, CPM router instance, or service ID

Values

router-instance : *router name* or *service-id*

router-name Base | management | *cpm-vr-name*

cpm-vr-name [32 characters maximum]

service-id 1 to 2147483647

Default Base

timeout *timeout* — specifies the timeout in seconds

Values 1 to 10

Default 5

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.

The following example is from a 7750 SR:

```
A:ALA-1>config>router>bgp>group# pwc
-----
Present Working Context :
-----
<root>
  configure
  router Base
  bgp
  group test
  ospf
  area 1
-----
A:ALA-1>config>router>bgp>group#
```

When the **previous** keyword is specified, the previous context displays. 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.

The following example is from a 7450 ESS:

```
*A:ALA-1>config>router>ospf>area>if# pwc previous
-----
Previous Working Context :
-----
<root>
  configure
  router "Base"
  ospf
  area "0.0.0.0"
-----
*A:ALA-1config>router>ospf>area>if#
```

Default	N/A
Parameters	previous — displays the previous present working context

sleep

Syntax	sleep [<i>seconds</i>]
Context	<global>
Description	This command causes the console session to pause operation (sleep) for 1 second (default) or for the specified number of seconds.
Default	sleep 1
Parameters	<i>seconds</i> — the number of seconds for the console session to sleep, expressed as a decimal integer
	Default 1
	Values 1 to 100

ssh

Syntax	ssh [<i>ip-addr</i> <i>dns-name</i> <i>username@ip-addr</i>] [- I <i>username</i>] [- v <i>SSH-version</i>] [router <i>router-instance</i>] service-name <i>service-name</i>]				
Context	<global>				
Description	<p>This 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 session, the SSH server must be operational.</p> <p>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 SSH session.</p>				
Default	N/A				
Parameters	<p><i>ip-address</i> / <i>host-name</i> — the remote host to open an SSH session to. The IP address or the DNS name (providing DNS name resolution is configured) can be specified.</p> <p><i>username</i> — the user name to use when opening the SSH session</p> <p>router <i>router-instance</i> — specifies the router name or service ID</p> <p>Values</p> <p><i>router-instance</i> : <i>router-name</i> or <i>vprn-svc-id</i></p> <table> <tr> <td><i>router-name</i></td><td>Base management vpls-management</td></tr> <tr> <td><i>vprn-svc-id</i></td><td>1 to 2147483647</td></tr> </table> <p>Default Base</p>	<i>router-name</i>	Base management vpls-management	<i>vprn-svc-id</i>	1 to 2147483647
<i>router-name</i>	Base management vpls-management				
<i>vprn-svc-id</i>	1 to 2147483647				

telnet

Syntax	telnet [<i>ip-address</i> <i>dns-name</i>] [<i>port</i>] [router <i>router-instance</i>]
Context	<global>
Description	This command opens a Telnet session to a remote host. Telnet servers in SR-series networks limit Telnet clients to three attempts to login; this number is not user configurable. The Telnet server disconnects the Telnet client session after three attempts.
Default	N/A
Parameters	<i>ip-address</i> — specifies the IP address or the DNS name (providing DNS name resolution is configured)

Values

<i>ipv4-address</i>	<i>a.b.c.d</i>	
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i>	<i>x</i> : [0 to FFFF]H
	<i>x:x:x:x:x:x:d.d.d.d[-interface]</i>	<i>d</i> : [0 to 255]D <i>ipv6-address</i>

Note: IPv6 applies to the 7750 SR and 7950 XRS.



dns-name — specifies the DNS name (if DNS name resolution is configured)

Values 128 characters maximum

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

Default 23

Values 1 to 65535

router *router-instance* — specifies the router name or service ID

Values

<i>router-instance</i> : <i>router-name</i> or <i>vprn-svc-id</i>	
<i>router-name</i>	Base management vpls-management
<i>vprn-svc-id</i>	1 to 2147483647

Default Base

traceroute

Syntax	<code>traceroute</code> { <i>ip-address</i> <i>dns-name</i> } [<i>tll tll</i>] [<i>wait milliseconds</i>] [<i>no-dns</i>] [<i>source ip-address</i>] [<i>tos type-of-service</i>] [<i>router router-instance</i>]																				
Context	<global>																				
Description	<p>The TCP/IP traceroute utility determines the route to a destination address. Note that aborting a traceroute with the <Ctrl-C> command could require issuing a second <Ctrl-C> command before the prompt is returned.</p> <pre>A:ALA-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 A:ALA-1#</pre>																				
Default	N/A																				
Parameters	<p><i>ip-address</i> <i>dns-name</i> — the remote address to traceroute. The IP address or the DNS name (if DNS name resolution is configured) can be specified.</p> <table><tr><td colspan="4">Values</td></tr><tr><td>ipv4-address</td><td>a.b.c.d</td><td colspan="2"></td></tr><tr><td>ipv6-address</td><td>x:x:x:x:x:x[-interface]</td><td>x:</td><td>[0 to FFFF]H</td></tr><tr><td></td><td>x:x:x:x:x:x:d.d.d.d[-interface]</td><td>d:</td><td>[0 to 255]D</td></tr><tr><td>dns-name</td><td>128 characters maximum</td><td colspan="2"></td></tr></table>	Values				ipv4-address	a.b.c.d			ipv6-address	x:x:x:x:x:x[-interface]	x:	[0 to FFFF]H		x:x:x:x:x:x:d.d.d.d[-interface]	d:	[0 to 255]D	dns-name	128 characters maximum		
Values																					
ipv4-address	a.b.c.d																				
ipv6-address	x:x:x:x:x:x[-interface]	x:	[0 to FFFF]H																		
	x:x:x:x:x:x:d.d.d.d[-interface]	d:	[0 to 255]D																		
dns-name	128 characters maximum																				



Note: IPv6 applies to the 7750 SR and 7950 XRS.

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

Values 1 to 255

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

Default 5000

Values 1 to 60000

no-dns — a DNS lookup for the specified host name will not be performed

Default DNS lookups are performed

source *ip-address* — the source IP address to use as the source of the probe packets in dotted decimal notation. If the IP address is not one of the device's interfaces, an error is returned.

tos *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 *router-instance* — specifies the router name, CPM router instance, or service ID

Values

router-instance : *router-name* or *service-id*

```
router-name      Base | management | cpm-vr-name
```

cpm-vr-name [32 characters maximum]

service-id 1 to 2147483647

Default	Base
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18
19	19
20	20
21	21
22	22
23	23
24	24
25	25
26	26
27	27
28	28
29	29
30	30
31	31
32	32
33	33
34	34
35	35
36	36
37	37
38	38
39	39
40	40
41	41
42	42
43	43
44	44
45	45
46	46
47	47
48	48
49	49
50	50
51	51
52	52
53	53
54	54
55	55
56	56
57	57
58	58
59	59
60	60
61	61
62	62
63	63
64	64
65	65
66	66
67	67
68	68
69	69
70	70
71	71
72	72
73	73
74	74
75	75
76	76
77	77
78	78
79	79
80	80
81	81
82	82
83	83
84	84
85	85
86	86
87	87
88	88
89	89
90	90
91	91
92	92
93	93
94	94
95	95
96	96
97	97
98	98
99	99
100	100

tree

Syntax **tree** [**detail**] [**flat**] [*command-string*]

Context <global>

Description	This command displays the command hierarchy structure of the current working context.
--------------------	---

Default N/A

Parameters **detail** — displays parameter information for each command shown in the tree output

flat — displays the full context on each line

command-string — displays the CLI command string (the CLI branch relative to the current CLI context)

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.
--------------------	---

Default N/A

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 — sends the *message-string* to all users logged into the router

message-string — the message string to send. Allowed values are any string up to 250 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

2.13.2.2 Monitor CLI Commands

card

Syntax	card <i>slot-number</i> fp <i>fp-number</i> ingress { access network } queue-group <i>queue-group-name</i> instance <i>instance-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] policer <i>policer-id</i> [absolute percent-rate <i>reference-rate</i>]
Context	monitor
Description	This command monitors policer statistics in an ingress FP queue group.
Default	N/A
Parameters	<p>card <i>slot-number</i> — specifies the slot number associated with the queue group, expressed as an integer</p> <p>Values 1 to 20</p> <p>fp <i>fp-number</i> — specifies the FP number associated with the queue group, expressed as an integer</p> <p>Values 1 to 2</p> <p>ingress — displays policer statistics applied on the ingress FP</p> <p>access — displays policer statistics on the FP access</p> <p>network — displays policer statistics on the FP network</p> <p>queue-group <i>queue-group-name</i> — specifies the name of the queue group up to 32 characters in length</p> <p>instance <i>instance-id</i> — specifies the identification of a specific instance of the queue-group</p> <p>Values 1 to 65535</p> <p>interval <i>interval</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p>

policer *policer-id* — must exist within the queue-group template applied to the ingress context of the forwarding plane

Values 1 to 8

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

percent-rate — rate-per-second for each statistic is displayed based on the reference rate of 10G

Default 10

Values 1 to 999

reference-rate — rate-per-second for each statistic is displayed as a percentage based on the reference rate specified

Values 100M, 1G, 10G, 40G, 100G, 400G

ccag

Syntax	ccag <i>ccag-id</i> [path { a b }] [type { sap-sap sap-net net-sap }] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor
Description	Displays monitor command output of traffic statistics for Cross Connect Aggregation Groups (CCAGs) ports.
Default	N/A
Parameters	<p><i>ccag-id</i> — specifies the CCAG instance to monitor</p> <p>path — specifies the CCA path nodal context where the CCA path bandwidth, buffer and accounting parameters are maintained. The path context must be specified with either the a or b keyword specifying the CCA path context to be entered.</p> <p>type — specifies cross connect type</p> <p>Values sap-sap, sap-net, net-sap</p> <p>interval — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

cpm-filter

Syntax	cpm-filter
Context	monitor
Description	This command displays monitor command output for CPM filters.
Default	N/A

ip

Syntax	ip entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>cpm-filter
Description	This command displays monitor command statistics for IP filter entries.
Default	N/A
Parameters	<p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 65535</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

ipv6

Syntax	ipv6 entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>cpm-filter
Description	This command displays monitor command statistics for IPv6 filter entries.

Parameters	<p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 65535</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>
-------------------	---

mac

Syntax	mac entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>cpm-filter
Description	This command displays monitor command statistics for MAC filter entries.
Parameters	<p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 65535</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

filter

Syntax	filter
---------------	---------------

Context	monitor
Description	This command enables the context to configure criteria to monitor IP and MAC filter statistics.

ip

Syntax	ip <i>ip-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>filter
Description	<p>This command enables IP filter monitoring. The statistical information for the specified IP filter entry displays at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified IP filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Parameters	<p><i>ip-filter-id</i> — displays detailed information for the specified filter ID and its filter entries</p> <p>Values 1 to 65535</p> <p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 65535</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

Output

Sample Output

```
A:ALA-1>monitor# filter ip 10 entry 1 interval 3 repeat 3 absolute
=====
```

```

Monitor statistics for IP filter 10 entry 1
=====
At time t = 0 sec (Base Statistics)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 3 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 6 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 9 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
=====
A:ALA-1>monitor#

```

```

A:ALA-1>monitor# filter ip 10 entry 1 interval 3 repeat 3 rate
=====
Monitor statistics for IP filter 10 entry 1
=====
At time t = 0 sec (Base Statistics)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 3 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 6 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 9 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
=====
A:ALA-1>monitor#

```

ipv6

Syntax	ipv6 <i>ipv6-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>filter
Description	<p>This command enables IPv6 filter monitoring. The statistical information for the specified IPv6 filter entry displays at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified IPv6 filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p>

When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

- Parameters**
- ipv6-filter-id* — displays detailed information for the specified IPv6 filter ID and its filter entries
 - Values** 1 to 65535
 - entry** *entry-id* — displays information on the specified IPv6 filter entry ID for the specified filter ID only
 - Values** 1 to 65535
 - interval** *seconds* — configures the interval for each display in seconds
 - Default** 5 seconds
 - Values** 3 to 60
 - repeat** *repeat* — configures how many times the command is repeated
 - Default** 10
 - Values** 1 to 999
 - absolute** — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.
 - rate** — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-48# monitor filter ipv6 100 entry 10 interval 3 repeat 3 absolute
=====
Monitor statistics for IPv6 filter 100 entry 10
-----
At time t = 0 sec (Base Statistics)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 3 sec (Mode: Absolute)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 6 sec (Mode: Absolute)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 9 sec (Mode: Absolute)
-----
Ing. Matches : 0                               Egr. Matches : 01
=====
A:ALA-48#
```

```
A:ALA-48# monitor filter ipv6 100 entry 10 interval 3 repeat 3 rate
=====
Monitor statistics for IPv6 filter 100 entry 10
-----
At time t = 0 sec (Base Statistics)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 3 sec (Mode: Rate)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 6 sec (Mode: Rate)
-----
Ing. Matches : 0                               Egr. Matches : 1
-----
At time t = 9 sec (Mode: Rate)
-----
Ing. Matches : 0                               Egr. Matches : 1
=====
A:ALA-48#
```

mac

Syntax	mac <i>mac-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>filter
Description	<p>This command enables MAC filter monitoring. The statistical information for the specified MAC filter entry displays at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified MAC filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p><i>mac-filter-id</i> — the MAC filter policy ID</p> <p>Values 1 to 65535</p> <p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 65535</p>

interval *seconds* — configures the interval for each display in seconds

Default 5 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta.

Output

Sample Output

```
A:ALA-1>monitor>filter# mac 50 entry 10 interval 3 repeat 3 absolute
=====
Monitor statistics for Mac filter 50 entry 10
=====
At time t = 0 sec (Base Statistics)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 3 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 6 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 9 sec (Mode: Absolute)
-----
Ing. Matches: 0                               Egr. Matches      : 0
=====

A:ALA-1>monitor>filter# mac 50 entry 10 interval 3 repeat 3 rate
=====
Monitor statistics for Mac filter 50 entry 10
=====
At time t = 0 sec (Base Statistics)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 3 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
At time t = 6 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
-----
```

```

At time t = 9 sec (Mode: Rate)
-----
Ing. Matches: 0                               Egr. Matches      : 0
=====
A:ALA-1>monitor>filter#

```

lag

Syntax	lag <i>lag-id</i> [<i>lag-id...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor
Description	<p>This command monitors traffic statistics for Link Aggregation Group (LAG) ports. Statistical information for the specified LAG ID(s) displays at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified LAG ID. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p><i>lag-id</i> — the number of the LAG</p> <p>Default none — the LAG ID value must be specified</p> <p>Values 1 to 800</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>
Output	

Sample Output

```
A:ALA-12# monitor lag 12
```

```
=====
Monitor statistics for LAG ID 12
=====
Port-id Input Input Output Output Input Output
Bytes Packets Bytes Packets Errors Errors
-----
At time t = 0 sec (Base Statistics)
-----
1/1/1 2168900 26450 64 1 0 0
1/1/2 10677318 125610 2273750 26439 0 0
1/1/3 2168490 26445 0 0 0 0
-----
Totals 15014708 178505 2273814 26440 0 0
-----
At time t = 5 sec (Mode: Delta)
-----
1/1/1 0 0 0 0 0 0
1/1/2 258 3 86 1 0 0
1/1/3 82 1 0 0 0 0
-----
Totals 340 4 86 1 0 0
=====
A:ALA-12#
```

management-access-filter

Syntax	management-access-filter
Context	monitor
Description	This command enables the context to monitor management-access filters. These filters are configured in the config>system>security>mgmt-access-filter context.
Default	N/A

ip

Syntax	ip entry <i>entry-id</i> [<i>interval seconds</i>] [<i>repeat repeat</i>] [<i>absolute</i> <i>rate</i>]
Context	monitor>management-access-filter
Description	This command monitors statistics for the MAF IP filter entry.
Default	N/A
Parameters	entry <i>entry-id</i> — specifies an existing IP MAF entry ID Values 1 to 9999 interval <i>seconds</i> — configures the interval for each display in seconds Default 10 Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

ipv6

Syntax **ipv6** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>management-access-filter

Description This command monitors statistics for the MAF IPv6 filter entry.

Default N/A

Parameters **entry** *entry-id* — specifies an existing IP MAF entry ID

Values 1 to 9999

interval seconds — configures the interval for each display in seconds

Default 10

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

mac

Syntax **mac** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>management-access-filter

Description This command monitors statistics for the MAF MAC filter entry.

Default N/A

Parameters **entry** *entry-id* — specifies an existing IP MAF entry ID

Values 1 to 9999

interval *seconds* — configures the interval for each display in seconds

Default 10

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

port

Syntax	port <i>port-id</i> [<i>port-id...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate] [multiclass]																													
Context	monitor																													
Description	<p>This command enables port traffic monitoring. The specified port(s) statistical information displays at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified port(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>																													
Default	N/A																													
Parameters	<p>port <i>port-id</i> — specifies up to 5 port IDs. Port-IDs are only MLPPP bundles or bundle protection groups when the multiclass is specified.</p> <table><tr><td><i>port-id</i></td><td><i>slot/mda/port</i> [.channel]</td><td></td></tr><tr><td>eth-sat-id</td><td>esat-id/<i>slot/port</i></td><td></td></tr><tr><td></td><td>esat</td><td>keyword</td></tr><tr><td></td><td><i>id</i></td><td>1 to 20</td></tr><tr><td>pxc-id</td><td>pxc-id.<i>sub-port</i></td><td></td></tr><tr><td></td><td>pxc</td><td>keyword</td></tr><tr><td></td><td><i>id</i></td><td>1 to 64</td></tr><tr><td></td><td><i>sub-port</i></td><td>a, b</td></tr><tr><td>aps-id</td><td>aps-group-id [.channel]</td><td></td></tr></table>			<i>port-id</i>	<i>slot/mda/port</i> [.channel]		eth-sat-id	esat-id / <i>slot/port</i>			esat	keyword		<i>id</i>	1 to 20	pxc-id	pxc-id . <i>sub-port</i>			pxc	keyword		<i>id</i>	1 to 64		<i>sub-port</i>	a, b	aps-id	aps-group-id [.channel]	
<i>port-id</i>	<i>slot/mda/port</i> [.channel]																													
eth-sat-id	esat-id / <i>slot/port</i>																													
	esat	keyword																												
	<i>id</i>	1 to 20																												
pxc-id	pxc-id . <i>sub-port</i>																													
	pxc	keyword																												
	<i>id</i>	1 to 64																												
	<i>sub-port</i>	a, b																												
aps-id	aps-group-id [.channel]																													

	aps	keyword
	<i>group-id</i>	1 to 64 (16 for 7750 SR-c12 and 7750 SR-c4)
bundle-id	bundle-type-slot/mda.bundle-num	
	bundle	keyword
	<i>type</i>	ima, ppp
	<i>bundle-num</i>	1 to 128 (16 for 7750 SR-c12 and 7750 SR-c4)

interval *seconds* — configures the interval for each display in seconds

Default 10 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12>monitor# port 2/1/4 interval 3 repeat 3 absolute
=====
Monitor statistics for Port 2/1/4
=====
                                     Input          Output
-----
At time t = 0 sec (Base Statistics)
-----
Octets                               0              0
Packets                             39             175
Errors                               0              0
-----
At time t = 3 sec (Mode: Absolute)
-----
Octets                               0              0
Packets                             39             175
Errors                               0              0
-----
At time t = 6 sec (Mode: Absolute)
-----
Octets                               0              0
Packets                             39             175
Errors                               0              0
-----
At time t = 9 sec (Mode: Absolute)
```



```

-----
Octets                                0                                0
Packets                              39                               175
Errors                                0                                0
=====
A:ALA-12>monitor#

A:ALA-12>monitor# port 2/1/4 interval 3 repeat 3 rate
=====
Monitor statistics for Port 2/1/4
=====
                                     Input                               Output
-----
At time t = 0 sec (Base Statistics)
-----
Octets                                0                                0
Packets                              39                               175
Errors                                0                                0
-----
At time t = 3 sec (Mode: Rate)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0
Bits                                  0                                0
Utilization (% of port capacity)      0.00                               0.00
-----
At time t = 6 sec (Mode: Rate)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0
Bits                                  0                                0
Utilization (% of port capacity)      0.00                               0.00
-----
At time t = 9 sec (Mode: Rate)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0
Bits                                  0                                0
Utilization (% of port capacity)      0.00                               0.00
=====
A:ALA-12>monitor#

=====
*A:Cpm-A> monitor port bundle-fr-1/1.1
=====
Monitor statistics for Port bundle-fr-1/1.1
=====
                                     Input                               Output
-----
At time t = 0 sec (Base Statistics)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0

```

port

Syntax	port all-ethernet-rates [<i>interval seconds</i>] [<i>repeat repeat</i>]
Context	monitor
Description	<p>This command enables port traffic monitoring and utilization output for all data Ethernet ports enabled in the system, in a table output format.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p>interval seconds — configures the interval for each display in seconds</p> <p>Default 10 seconds</p> <p>Values 3 to 60</p> <p>repeat repeat — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p>

Output

Sample Output

```
A:ALA-12>monitor# port all-ethernet-rates interval 3 repeat 100
=====
Monitor statistics for all Ethernet Port Rates
=====
Port-Id          D              Bits   Packets   Errors   Util
-----
At time t = 0 sec (Base Statistics)
-----
5/1/1            I              0       0         0       0.00
                  O              0       0         0       0.00
5/2/1            I              0       0         0       0.00
                  O              0       0         0       0.00
-----
At time t = 3 sec (Mode: Rate)
-----
5/1/1            I              0       0         0       0.00
                  O              0       0         0       0.00
5/2/1            I              0       0         0       0.00
                  O              0       0         0       0.00
-----
At time t = 6 sec (Mode: Rate)
-----
```

```

5/1/1      I      0      0      0      0.00
           O      0      0      0      0.00

5/2/1      I      0      0      0      0.00
           O      0      0      0      0.00

```

At time t = 9 sec (Mode: Rate)

```

5/1/1      I      4286480384  697669      0      43.98
           I      4286382080  697653      0      43.98

5/2/1      I      4254070784  692394      0      43.64
           I      4253952000  692375      0      43.64

```

At time t = 12 sec (Mode: Rate)

```

5/1/1      I      9746288640  1586K      0      99.99
           I      9746216960  1586K      0      99.99

5/2/1      I      9746280448  1586K      0      99.99
           I      9746167808  1586K      0      99.99

```

=====

A:ALA-12>monitor#

atm

- Syntax** `atm [interval seconds] [repeat repeat] [absolute | rate]`
- Context** monitor>port
- Description** This command enables ATM port traffic monitoring.
- Default** N/A
- Parameters**
- interval seconds** — configures the interval for each display in seconds
 - Default** 10 seconds
 - Values** 3 to 60
 - repeat repeat** — configures how many times the command is repeated
 - Default** 10
 - Values** 1 to 999
 - absolute** — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.
 - rate** — rate-per-second for each statistic is displayed instead of the delta

port

Syntax **port** *port-id* **atm** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm aal-5** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm ilmi** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm interface-connection** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm pvc** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm pvp** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
port *port-id* **atm pvt** [*interval seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors ATM port traffic statistics.

Default N/A

Parameters *port-id* — specifies up to 5 port IDs

Values

<i>port-id</i>	<i>slot/mda/port [.channel]</i>		
eth-sat-id	esat-id / <i>slot/port</i>		
	esat	keyword	
	<i>id</i>	1 to 20	
pxc-id	pxc-id . <i>sub-port</i>		
	pxc	keyword	
	<i>id</i>	1 to 64	
	<i>sub-port</i>	a, b	
aps-id	aps-group-id [<i>.channel</i>]		
	aps	keyword	
	<i>group-id</i>	1 to 64	
bundle-id	bundle-type-slot/mda.bundle-num		
	bundle	keyword	
	<i>type</i>	ima, ppp	
	<i>bundle-num</i>	1 to 128	

atm — keyword specifying ATM information

interface-connection — monitors ATM interface statistics

interval *seconds* — configures the interval for each display in seconds

Default 5 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

Default default mode delta

rate — rate-per-second for each statistic is displayed instead of the delta

Default default mode delta

aal-5 — displays ATM Adaptation Layer 5 (AAL5) information

ilmi — monitors ATM ILMI statistics

pvc — identifies the port by the PVC identifier (vpi/vci)

pvp — identifies the port by the permanent virtual path

pvt — identifies the port by the permanent virtual tunnel

oam — identifies the port by the OAM test suite ID

qos

Syntax	qos
Context	monitor
Description	This command enables the context to configure criteria to monitor QoS scheduler statistics for specific customers and SAPs.
Default	N/A

arbiter-stats

Syntax	arbiter-stats
Context	monitor>qos
Description	This command enables the context to configure monitor commands for arbiter statistics.
Default	N/A

card

Syntax	card <i>slot-number</i> fp <i>fp-number</i> queue-group <i>queue-group-name</i> instance <i>instance-id</i> [ingress] [access networks] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute percent-rate <i>reference-rate</i>] [arbiter <i>root</i> <i>name</i>]
Context	monitor>qos>arbiter-stats
Description	This command monitors arbiter statistics in an ingress FP queue group.

Default	N/A
Parameters	<p>card <i>slot-number</i> — specifies the slot number associated with the queue group, expressed as an integer</p> <p>Values 1 to 20</p> <p>fp <i>fp-number</i> — specifies the FP number associated with the queue group, expressed as an integer</p> <p>Values 1 to 2</p> <p>queue-group <i>queue-group-name</i> — specifies the name of the queue group up to 32 characters in length</p> <p>instance <i>instance-id</i> — specifies the identification of a specific instance of the queue-group</p> <p>Values 1 to 65535</p> <p>ingress — displays arbiter-name statistics applied on the ingress FP</p> <p>access — displays arbiter-name statistics applied on the FP access</p> <p>network — displays arbiter-name statistics applied on the FP network</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>percent-rate — rate-per-second for each statistic is displayed based on the reference rate of 10G</p> <p>reference-rate — rate-per-second for each statistic is displayed as a percentage based on the reference rate specified</p> <p>Values 100M, 1G, 10G, 40G, 100G, 400G</p> <p>arbiter <i>name</i> — specifies the name of the policer control policy arbiter</p> <p>Values an existing arbiter-name in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>root — specifies the root arbiter</p>

customer

Syntax	customer <i>customer-id</i> site <i>customer-site-name</i> [arbiter <i>root</i> <i>name</i>] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>arbiter-stats
Description	This command monitors arbiter statistics for a customer site.
Default	N/A
Parameters	<p><i>customer-id</i> — specifies the ID number to be associated with the customer, expressed as an integer</p> <p>Values 1 to 2147483647</p> <p>site <i>customer-site-name</i> — specifies the customer site which is an anchor point for ingress and egress arbiter hierarchy</p> <p>arbiter <i>name</i> — specifies the name of the policer control policy arbiter. This parameter is mandatory if the SAP resides on a LAG in adapt-qos link or port-fair mode.</p> <p>Values an existing arbiter-name in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p><i>root</i> — specifies the root arbiter</p> <p>ingress — displays arbiter-name statistics applied on the site ingress</p> <p>egress — displays arbiter-name statistics applied on the site egress</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed</p>

port

Syntax	port <i>port-id</i> egress <i>network</i> queue-group <i>queue-group-name</i> instance <i>instance-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate] [arbiter <i>root</i> <i>name</i>]
---------------	---

Context	monitor>qos>arbiter-stats
Description	This command monitors arbiter statistics for a customer site.
Default	N/A
Parameters	<p>port <i>port-id</i> — specifies the port ID</p> <p>Values <i>slot/mda/port</i> <i>esat-id/slot/port</i> <i>pxc-id.sub-port</i></p> <p>egress <i>network</i> — specifies statistics for an egress network queue group</p> <p>Values <i>network</i></p> <p>queue-group <i>queue-group-name</i> — specifies the name of the queue group up to 32 characters in length</p> <p>instance <i>instance-id</i> — specifies the identification of a specific instance of the queue-group</p> <p>Values 1 to 65535</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Values 11 to 60</p> <p>Default 11 seconds</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Values 1 to 999</p> <p>Default 10</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed</p> <p>arbiter <i>name</i> — specifies the name of the policer control policy arbiter</p> <p>Values an existing arbiter-name in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>root — specifies the root arbiter</p>

sap

Syntax	sap <i>sap-id</i> [arbiter <i>name</i> <i>root</i>] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>arbiter-stats

Description	This command monitors arbiter statistics for a SAP.
Default	N/A
Parameters	<p><i>sap-id</i> — specifies the physical port identifier portion of the SAP definition</p> <p>arbiter <i>name</i> — specifies the name of the policer control policy arbiter. This parameter is mandatory if the SAP resides on a LAG in adapt-qoslink or port-fair mode.</p> <p>Values an existing <i>scheduler-name</i> in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>root — specifies the arbiter to which this queue would be feeding</p> <p>ingress — displays <i>scheduler-name</i> statistics applied on the ingress SAP</p> <p>egress — displays <i>scheduler-name</i> statistics applied on the egress SAP</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

subscriber

Syntax	subscriber <i>sub-ident-string</i> [arbiter <i>name</i> root] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>arbiter-stats
Description	This command monitors arbiter statistics for a subscriber.
Default	N/A
Parameters	<i>sub-ident-string</i> — specifies an existing subscriber a identification policy name

arbiter *name* — specifies the name of the policer control policy arbiter

Values an existing arbiter name in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

root — specifies the arbiter to which this queue would be feeding

ingress — displays arbiter name statistics applied on the ingress SAP

egress — displays arbiter name statistics applied on the egress SAP

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

port

Syntax **port** *port-id* **exp-secondary-shaper** *shaper-name* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>qos

Description This command monitors expanded secondary shaper statistics.

Default N/A

Parameters **port** *port-id* — specifies the port ID

Values *slot/mda/port*
esat-id/slot/port
pxc-id.sub-port

exp-secondary-shaper *shaper-name* — displays statistics for the named exp secondary shaper

interval — *seconds* — configures the interval for each display in seconds.

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed

port

Syntax **port** *port-id* **vport** *name* **monitor-threshold** [*interval seconds*] [**repeat** *repeat*]

Context monitor>qos

Description This command monitors VPORT statistics.

Default N/A

Parameters **port** *port-id* — specifies the port ID

Values *slot/mda/port [.channel]*
esat-id/slot/port
pxc-id.sub-port

vport *name* — displays statistics for the named VPORT

monitor-threshold — displays the exceed-count for the port-scheduler for the named VPORT

interval — *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

scheduler-stats

Syntax **scheduler-stats**

Context monitor>qos

Description This command enables the context to configure monitor commands for scheduler statistics.

Default N/A

customer

Syntax	customer <i>customer-id</i> site <i>customer-site-name</i> [scheduler <i>scheduler-name</i>] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>scheduler-stats
Description	<p>Use this command to monitor scheduler statistics per customer multi-service-site. The first screen displays the current statistics related to the specified customer ID and customer site name. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. These commands display selected statistics per the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p><i>customer-id</i> — specifies the ID number to be associated with the customer, expressed as an integer</p> <p>Values 1 to 2147483647</p> <p>site <i>customer-site-name</i> — specifies the customer site which is an anchor point for ingress and egress virtual scheduler hierarchy</p> <p>scheduler <i>scheduler-name</i> — specifies an existing <i>scheduler-name</i>. Scheduler names are configured in the config>qos>scheduler-policy>tier level context. This parameter is mandatory if the customer resides on a LAG in adapt-qoslink or port-fair mode.</p> <p>Values an existing <i>scheduler-name</i> is in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>ingress — displays the customer's multi-service-site ingress scheduler policy</p> <p>egress — displays the customer's multi-service-site egress scheduler policy</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

port

Syntax	port <i>port-id</i> queue-group <i>queue-group-name</i> [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate] [access network] [instance <i>instance-id</i>]
Context	monitor>qos>scheduler-stats
Description	This command monitors scheduler statistics in a port queue group.
Default	N/A
Parameters	<p>port <i>port-id</i> — specifies the port ID</p> <p>Values <i>slot/mda/port</i> <i>esat-id/slot/port</i> <i>pxc-id.sub-port</i></p> <p>queue-group <i>queue-group-name</i> — specifies the name of the queue group up to 32 characters in length</p> <p>instance <i>instance-id</i> — specifies the identification of a specific instance of the queue-group</p> <p>Values 1 to 65535</p> <p>ingress — specifies statistics are for an ingress queue group</p> <p>egress — specifies statistics are for an egress queue group</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed</p> <p>access — displays scheduler statistics applied on an access port</p> <p>network — displays scheduler statistics applied on a network port</p>

port

Syntax	port <i>port-id</i> vport <i>name</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>scheduler-stats

Description	This command monitors scheduler statistics in a VPORT.
Default	N/A
Parameters	<p>port <i>port-id</i> — specifies the port ID</p> <p>Values <i>slot/mda/port</i> <i>esat-id/slot/port</i> <i>pxc-id.sub-port</i></p> <p>vport <i>name</i> — displays statistics for the named VPORT</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed</p>

sap

Syntax	sap <i>sap-id</i> [scheduler <i>scheduler-name</i>] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>scheduler-stats
Description	<p>Use this command to monitor scheduler statistics for a SAP at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified SAP. The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition

scheduler *scheduler-name* — specifies an existing *scheduler-name*. Scheduler names are configured in the **config>qos>scheduler-policy>tier** *level* context. This parameter is mandatory if the SAP resides on a LAG in adapt-qoslink or port-fair mode.

Values an existing *scheduler-name* in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

ingress — displays *scheduler-name* statistics applied on the ingress SAP

egress — displays *scheduler-name* statistics applied on the egress SAP

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

sap

Syntax	sap <i>sap-id</i> encap-group <i>group-name</i> [member <i>encap-id</i>] [scheduler <i>scheduler-name</i>] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>scheduler-stats
Description	This command monitors scheduler statistics for a SAP encap-group.
Default	N/A
Parameters	<p>sap <i>sap-id</i> — specifies the physical port identifier portion of the SAP definition</p> <p>encap-group <i>group-name</i> — displays statistics for the encap group</p> <p>member <i>encap-id</i> — the value of the encap-id to be displayed</p> <p>Values 0 to 16777215</p>

scheduler *scheduler-name* — specifies an existing scheduler-name. Scheduler names are configured in the **config>qos>scheduler-policy>tier** level context. This parameter is mandatory if the SAP resides on a LAG in adapt-qoslink or port-fair mode

Values an existing scheduler-name is in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters.

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed

subscriber

Syntax	subscriber <i>sub-ident-string</i> [scheduler <i>scheduler-name</i>] [ingress egress] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>qos>scheduler-stats
Description	This command monitors scheduler statistics for a subscriber.
Default	N/A
Parameters	<p><i>sub-ident-string</i> — specifies an existing subscriber an identification policy name</p> <p>scheduler <i>scheduler-name</i> — specifies an existing QoS scheduler policy name. Scheduler names are configured in the config>qos>scheduler-policy>tier level context.</p> <p>Values an existing <i>scheduler-name</i> in the form of a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>ingress — displays <i>scheduler-name</i> statistics applied on the ingress SAP</p> <p>egress — displays <i>scheduler-name</i> statistics applied on the egress SAP</p>

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

subscriber

Syntax	subscriber <i>sub-ident-string</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate] sap <i>sap-id</i> sla-profile <i>sla-profile-name</i>
Context	monitor>qos>scheduler-stats
Description	This command monitors scheduler statistics for an SLA profile.
Default	N/A
Parameters	<p>subscriber <i>sub-ident-string</i> — specifies an existing subscriber an identification policy name</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed</p> <p>sap <i>sap-id</i> — specifies the physical port identifier portion of the SAP definition</p> <p>sla-profile <i>sla-profile-name</i> — specifies the SLA profile belonging to the subscriber host</p>

router

Syntax **router** [*router-instance*]

Context	monitor
Description	This command enables the context to configure criteria to monitor statistical information for a variety of routing protocols.
Default	N/A
Parameters	<i>router-instance</i> — specifies the router name or service ID
	Values
	<i>router-name:</i> Base, management
	<i>service-id:</i> 1 to 2147483647
	Default Base

neighbor

Syntax	neighbor <i>ip-address</i> [<i>ip-address...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>bgp
Description	<p>This command displays statistical BGP neighbor information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified neighbor(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Parameters	<p>neighbor <i>ip-address</i> — displays damping information for entries received from the BGP neighbor. Up to 5 IP addresses can be specified.</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p>

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12>monitor>router>bgp# neighbor 180.0.0.10 interval 3 repeat 3 absolute
=====
Monitor statistics for BGP Neighbor 180.0.0.10
=====
At time t = 0 sec
-----
Recd. Prefixes   : 2                Sent Prefixes    : 0
Recd. Paths      : 0                Suppressed Paths : 0
Num of Flaps     : 0
i/p Messages     : 916              o/p Messages     : 916
i/p Octets       : 17510            o/p Octets       : 17386
i/p Updates      : 2                o/p Updates      : 0
-----
At time t = 3 sec
-----
Recd. Prefixes   : 0                Sent Prefixes    : 0
Recd. Paths      : 0                Suppressed Paths : 0
Num of Flaps     : 0
i/p Messages     : 0                o/p Messages     : 0
i/p Octets       : 0                o/p Octets       : 0
i/p Updates      : 0                o/p Updates      : 0
-----
At time t = 6 sec
-----
Recd. Prefixes   : 0                Sent Prefixes    : 0
Recd. Paths      : 0                Suppressed Paths : 0
Num of Flaps     : 0
i/p Messages     : 0                o/p Messages     : 0
i/p Octets       : 0                o/p Octets       : 0
i/p Updates      : 0                o/p Updates      : 0
-----
At time t = 9 sec
-----
Recd. Prefixes   : 0                Sent Prefixes    : 0
Recd. Paths      : 0                Suppressed Paths : 0
Num of Flaps     : 0
i/p Messages     : 0                o/p Messages     : 0
i/p Octets       : 6                o/p Octets       : 0
i/p Updates      : 0                o/p Updates      : 0
=====
A:ALA-12>monitor>router>bgp#
```

statistics

Syntax **statistics** [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>router>isis

Description This command displays statistical IS-IS traffic information at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the specified router statistics. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

Default N/A

Parameters **interval** *seconds* — configures the interval for each display in seconds

Default 5 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12>monitor>router>isis# statistics interval 3 repeat 2 absolute
=====
ISIS Statistics
=====
At time t = 0 sec (Base Statistics)
-----
ISIS Instance      : 1                SPF Runs          : 2
Purge Initiated    : 0                LSP Regens.       : 11

CSPF Statistics

Requests           : 0                Request Drops     : 0
Paths Found        : 0                Paths Not Found   : 0
-----
PDU Type   Received   Processed   Dropped    Sent      Retransmitted
-----
LSP         0           0           0          0          0
IIH         0           0           0          74         0
CSNP        0           0           0          0          0
PSNP        0           0           0          0          0
Unknown     0           0           0          0          0
-----
```

At time t = 3 sec (Mode: Absolute)

```
-----
ISIS Instance      : 1                      SPF Runs          : 2
Purge Initiated    : 0                      LSP Regens.       : 11
```

CSPF Statistics

```
Requests           : 0                      Request Drops     : 0
Paths Found        : 0                      Paths Not Found   : 0
```

```
-----
PDU Type   Received   Processed   Dropped    Sent      Retransmitted
-----
LSP         0          0          0          0          0
IIH         0          0          0          74         0
CSNP        0          0          0          0          0
PSNP        0          0          0          0          0
Unknown     0          0          0          0          0
-----
```

At time t = 6 sec (Mode: Absolute)

```
-----
ISIS Instance      : 1                      SPF Runs          : 2
Purge Initiated    : 0                      LSP Regens.       : 11
```

CSPF Statistics

```
Requests           : 0                      Request Drops     : 0
Paths Found        : 0                      Paths Not Found   : 0
```

```
-----
PDU Type   Received   Processed   Dropped    Sent      Retransmitted
-----
LSP         0          0          0          0          0
IIH         0          0          0          74         0
CSNP        0          0          0          0          0
PSNP        0          0          0          0          0
Unknown     0          0          0          0          0
=====
```

A:ALA-12>monitor>router>isis# statistics interval 3 repeat 2 rate

ISIS Statistics

At time t = 0 sec (Base Statistics)

```
-----
ISIS Instance      : 1                      SPF Runs          : 2
Purge Initiated    : 0                      LSP Regens.       : 11
```

CSPF Statistics

```
Requests           : 0                      Request Drops     : 0
Paths Found        : 0                      Paths Not Found   : 0
```

```
-----
PDU Type   Received   Processed   Dropped    Sent      Retransmitted
-----
LSP         0          0          0          0          0
IIH         0          0          0          76         0
CSNP        0          0          0          0          0
PSNP        0          0          0          0          0
Unknown     0          0          0          0          0
```

```

-----
At time t = 3 sec (Mode: Rate)
-----
ISIS Instance      : 1                      SPF Runs          : 0
Purge Initiated    : 0                      LSP Regens.       : 0

CSPF Statistics

Requests           : 0                      Request Drops     : 0
Paths Found        : 0                      Paths Not Found   : 0
-----
PDU Type   Received   Processed   Dropped   Sent       Retransmitted
-----
LSP         0          0           0         0           0
IIH         0          0           0         0           0
CSNP        0          0           0         0           0
PSNP        0          0           0         0           0
Unknown     0          0           0         0           0
-----
At time t = 6 sec (Mode: Rate)
-----
ISIS Instance      : 1                      SPF Runs          : 0
Purge Initiated    : 0                      LSP Regens.       : 0

CSPF Statistics

Requests           : 0                      Request Drops     : 0
Paths Found        : 0                      Paths Not Found   : 0
-----
PDU Type   Received   Processed   Dropped   Sent       Retransmitted
-----
LSP         0          0           0         0           0
IIH         0          0           0         1           0
CSNP        0          0           0         0           0
PSNP        0          0           0         0           0
Unknown     0          0           0         0           0
=====
A:ALA-12>monitor>router>isis#

```

session

- Syntax** `session ldp-id [ldp-id...(up to 5 max)] [interval seconds] [repeat repeat] [absolute | rate]`
- Context** `monitor>router>ldp`
- Description** This command displays statistical information for LDP sessions at the configured interval until the configured count is reached.
- The first screen displays the current statistics related to the specified LDP session(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.
- When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

Default N/A

Parameters *ldp-id* — specifies the IP address of the LDP session to display

Values *ip-address[:label-space]*
ip-address — a.b.c.d
label-space — [0 to 65535]

interval *seconds* — configures the interval for each display in seconds

Default 5 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-103>monitor>router>ldp# session 10.10.10.104 interval 3 repeat 3 absolute
=====
Monitor statistics for LDP Session 10.10.10.104
=====
```

	Sent	Received

At time t = 0 sec (Base Statistics)		

FECs	1	2
Hello	5288	5289
Keepalive	8225	8225
Init	1	1
Label Mapping	1	4
Label Request	0	0
Label Release	0	0
Label Withdraw	0	0
Label Abort	0	0
Notification	0	0
Address	1	1
Address Withdraw	0	0

At time t = 3 sec (Mode: Absolute)		

FECs	1	2
Hello	5288	5289

Keepalive	8226	8226
Init	1	1
Label Mapping	1	4
Label Request	0	0
Label Release	0	0
Label Withdraw	0	0
Label Abort	0	0
Notification	0	0
Address	1	1
Address Withdraw	0	0

At time t = 6 sec (Mode: Absolute)

FECs	1	2
Hello	5288	5290
Keepalive	8226	8226
Init	1	1
Label Mapping	1	4
Label Request	0	0
Label Release	0	0
Label Withdraw	0	0
Label Abort	0	0
Notification	0	0
Address	1	1
Address Withdraw	0	0

At time t = 9 sec (Mode: Absolute)

FECs	1	2
Hello	5288	5290
Keepalive	8226	8226
Init	1	1
Label Mapping	1	4
Label Request	0	0
Label Release	0	0
Label Withdraw	0	0
Label Abort	0	0
Notification	0	0
Address	1	1
Address Withdraw	0	0

=====

A:ALA-12>monitor>router>ldp# session 10.10.10.104 interval 3 repeat 3 rate

=====

Monitor statistics for LDP Session 10.10.10.104

=====

Sent

Received

At time t = 0 sec (Base Statistics)

FECs	1	2
Hello	5289	5290
Keepalive	8227	8227
Init	1	1
Label Mapping	1	4
Label Request	0	0
Label Release	0	0


```

Label Withdraw          0          0
Label Abort             0          0
Notification            0          0
Address                 1          1
Address Withdraw        0          0
-----
At time t = 3 sec (Mode: Rate)
-----
FECs                    0          0
Hello                   0          0
Keepalive               0          0
Init                    0          0
Label Mapping           0          0
Label Request           0          0
Label Release           0          0
Label Withdraw          0          0
Label Abort             0          0
Notification            0          0
Address                 0          0
Address Withdraw        0          0
-----
At time t = 6 sec (Mode: Rate)
-----
FECs                    0          0
Hello                   0          0
Keepalive               0          0
Init                    0          0
Label Mapping           0          0
Label Request           0          0
Label Release           0          0
Label Withdraw          0          0
Label Abort             0          0
Notification            0          0
Address                 0          0
Address Withdraw        0          0
-----
At time t = 9 sec (Mode: Rate)
-----
FECs                    0          0
Hello                   0          0
Keepalive               0          0
Init                    0          0
Label Mapping           0          0
Label Request           0          0
Label Release           0          0
Label Withdraw          0          0
Label Abort             0          0
Notification            0          0
Address                 0          0
Address Withdraw        0          0
=====
A:ALA-12>monitor>router>ldp#

```

statistics

Syntax **statistics** [*interval seconds*] [*repeat repeat*] [*absolute | rate*]

Context	monitor>router>ldp
Description	<p>Monitor statistics for LDP instance at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the LDP statistics. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p style="padding-left: 40px;">Default 5 seconds</p> <p style="padding-left: 40px;">Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p style="padding-left: 40px;">Default 10</p> <p style="padding-left: 40px;">Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>
Output	

Sample Output

```
A:ALA-12>monitor>router>ldp# statistics interval 3 repeat 3 absolute
=====
Monitor statistics for LDP instance
=====
At time t = 0 sec (Base Statistics)
-----
Addr FECs Sent   : 0                      Addr FECs Recv   : 0
Serv FECs Sent   : 1                      Serv FECs Recv   : 2
-----
At time t = 3 sec (Mode: Absolute)
-----
Addr FECs Sent   : 0                      Addr FECs Recv   : 0
Serv FECs Sent   : 1                      Serv FECs Recv   : 2
-----
At time t = 6 sec (Mode: Absolute)
-----
Addr FECs Sent   : 0                      Addr FECs Recv   : 0
Serv FECs Sent   : 1                      Serv FECs Recv   : 2
-----
At time t = 9 sec (Mode: Absolute)
```

```
-----
Addr FECs Sent      : 0                      Addr FECs Recv      : 0
Serv FECs Sent      : 1                      Serv FECs Recv      : 2
=====
A:ALA-12>monitor>router>ldp#

A:ALA-12>monitor>router>ldp# statistics interval 3 repeat 3 rate
=====
Monitor statistics for LDP instance
=====
At time t = 0 sec (Base Statistics)
-----
Addr FECs Sent      : 0                      Addr FECs Recv      : 0
Serv FECs Sent      : 1                      Serv FECs Recv      : 2
-----
At time t = 3 sec (Mode: Rate)
-----
Addr FECs Sent      : 0                      Addr FECs Recv      : 0
Serv FECs Sent      : 0                      Serv FECs Recv      : 0
-----
At time t = 6 sec (Mode: Rate)
-----
Addr FECs Sent      : 0                      Addr FECs Recv      : 0
Serv FECs Sent      : 0                      Serv FECs Recv      : 0
-----
At time t = 9 sec (Mode: Rate)
-----
Addr FECs Sent      : 0                      Addr FECs Recv      : 0
Serv FECs Sent      : 0                      Serv FECs Recv      : 0
=====
A:ALA-12>monitor>router>ldp#
```

interface

Syntax	interface <i>interface</i> [<i>interface...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>mpls
Description	<p>This command displays statistics for MPLS interfaces at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the MPLS interface(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A

Parameters *interface* — specifies the IP address of the interface (*ip-address*) or interface name (*ip-int-name*). Up to 5 interfaces can be specified. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12>monitor>router>mpls# interface system interval 3 repeat 3 absolute
=====
Monitor statistics for MPLS Interface "system"
=====
At time t = 0 sec (Base Statistics)
-----
Transmitted : Pkts - 0          Octets - 0
Received    : Pkts - 0          Octets - 0
-----
At time t = 3 sec (Mode: Absolute)
-----
Transmitted : Pkts - 0          Octets - 0
Received    : Pkts - 0          Octets - 0
-----
At time t = 6 sec (Mode: Absolute)
-----
Transmitted : Pkts - 0          Octets - 0
Received    : Pkts - 0          Octets - 0
-----
At time t = 9 sec (Mode: Absolute)
-----
Transmitted : Pkts - 0          Octets - 0
Received    : Pkts - 0          Octets - 0
=====
A:ALA-12>monitor>router>mpls#

A:ALA-12>monitor>router>mpls# interface system interval 3 repeat 3 rate
=====
Monitor statistics for MPLS Interface "system"
=====
-----
Transmitted : Pkts - 0          Octets - 0
```

```
Received      : Pkts - 0                      Octets - 0
-----
At time t = 3 sec (Mode: Rate)
-----
Transmitted   : Pkts - 0                      Octets - 0
Received      : Pkts - 0                      Octets - 0
-----
At time t = 6 sec (Mode: Rate)
-----
Transmitted   : Pkts - 0                      Octets - 0
Received      : Pkts - 0                      Octets - 0
-----
At time t = 9 sec (Mode: Rate)
-----
Transmitted   : Pkts - 0                      Octets - 0
Received      : Pkts - 0                      Octets - 0
=====
A:ALA-12>monitor>router>mpls#
```

lsp-egress-stats

Syntax	lsp-egress-stats <i>lsp-name</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>mpls
Description	This command displays egress statistics for LSP interfaces at the configured interval until the configured count is reached.
Default	no lsp-egress-stats
Parameters	repeat <i>repeat</i> — specifies how many times the command is repeated Values 10 Values 1 to 999 interval <i>seconds</i> — specifies the interval for each display, in seconds Values 10 Values 3 to 60 absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics. rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
B:Dut-C-cpm2# monitor router mpls lsp-egress-stats sample repeat 3 interval 10
absolute
=====
Monitor egress statistics for MPLS LSP "sample"
-----
```

At time t = 0 sec (Base Statistics)

LSP Name : sample

Collect Stats : Enabled	Accting Plcy. : 5
Adm State : Up	PSB Match : True
FC BE	
InProf Pkts : 0	OutProf Pkts : 551
InProf Octets : 0	OutProf Octets: 560918
FC L2	
InProf Pkts : 0	OutProf Pkts : 551
InProf Octets : 0	OutProf Octets: 560918
FC AF	
InProf Pkts : 551	OutProf Pkts : 0
InProf Octets : 560918	OutProf Octets: 0
FC L1	
InProf Pkts : 551	OutProf Pkts : 0
InProf Octets : 560918	OutProf Octets: 0
FC H2	
InProf Pkts : 0	OutProf Pkts : 551
InProf Octets : 0	OutProf Octets: 560918
FC EF	
InProf Pkts : 0	OutProf Pkts : 551
InProf Octets : 0	OutProf Octets: 560918
FC H1	
InProf Pkts : 0	OutProf Pkts : 551
InProf Octets : 0	OutProf Octets: 560918
FC NC	
InProf Pkts : 551	OutProf Pkts : 0
InProf Octets : 560918	OutProf Octets: 0

At time t = 10 sec (Mode: Absolute)
-----LSP Name : sample

Collect Stats : Enabled	Accting Plcy. : 5
Adm State : Up	PSB Match : True
FC BE	
InProf Pkts : 0	OutProf Pkts : 580
InProf Octets : 0	OutProf Octets: 590440
FC L2	
InProf Pkts : 0	OutProf Pkts : 580
InProf Octets : 0	OutProf Octets: 590440
FC AF	
InProf Pkts : 580	OutProf Pkts : 0
InProf Octets : 590440	OutProf Octets: 0
FC L1	
InProf Pkts : 580	OutProf Pkts : 0
InProf Octets : 590440	OutProf Octets: 0
FC H2	
InProf Pkts : 0	OutProf Pkts : 580
InProf Octets : 0	OutProf Octets: 590440
FC EF	
InProf Pkts : 0	OutProf Pkts : 580
InProf Octets : 0	OutProf Octets: 590440
FC H1	
InProf Pkts : 0	OutProf Pkts : 580
InProf Octets : 0	OutProf Octets: 590440
FC NC	

```

InProf Pkts   : 580                      OutProf Pkts   : 0
InProf Octets : 590440                  OutProf Octets: 0
-----
At time t = 20 sec (Mode: Absolute)
-----
LSP Name      : sample
-----
Collect Stats : Enabled                  Accting Plcy. : 5
Adm State     : Up                      PSB Match    : True
FC BE
InProf Pkts   : 0                      OutProf Pkts   : 609
InProf Octets : 0                      OutProf Octets: 619962
FC L2
InProf Pkts   : 0                      OutProf Pkts   : 609
InProf Octets : 0                      OutProf Octets: 619962
FC AF
InProf Pkts   : 609                    OutProf Pkts   : 0
InProf Octets : 619962                OutProf Octets: 0
FC L1
InProf Pkts   : 609                    OutProf Pkts   : 0
InProf Octets : 619962                OutProf Octets: 0
FC H2
InProf Pkts   : 0                      OutProf Pkts   : 609
InProf Octets : 0                      OutProf Octets: 619962
FC EF
InProf Pkts   : 0                      OutProf Pkts   : 609
InProf Octets : 0                      OutProf Octets: 619962
FC H1
InProf Pkts   : 0                      OutProf Pkts   : 609
InProf Octets : 0                      OutProf Octets: 619962
FC NC
InProf Pkts   : 609                    OutProf Pkts   : 0
InProf Octets : 619962                OutProf Octets: 0
-----
At time t = 30 sec (Mode: Absolute)
-----
LSP Name      : sample
-----
Collect Stats : Enabled                  Accting Plcy. : 5
Adm State     : Up                      PSB Match    : True
FC BE
InProf Pkts   : 0                      OutProf Pkts   : 638
InProf Octets : 0                      OutProf Octets: 649484
FC L2
InProf Pkts   : 0                      OutProf Pkts   : 638
InProf Octets : 0                      OutProf Octets: 649484
FC AF
InProf Pkts   : 638                    OutProf Pkts   : 0
InProf Octets : 649484                OutProf Octets: 0
FC L1
InProf Pkts   : 638                    OutProf Pkts   : 0
InProf Octets : 649484                OutProf Octets: 0
FC H2
InProf Pkts   : 0                      OutProf Pkts   : 638
InProf Octets : 0                      OutProf Octets: 649484
FC EF
InProf Pkts   : 0                      OutProf Pkts   : 638
InProf Octets : 0                      OutProf Octets: 649484
FC H1

```

```

InProf Pkts   : 0
InProf Octets : 0
FC NC
InProf Pkts   : 638
InProf Octets : 649484
OutProf Pkts  : 638
OutProf Octets: 649484
=====
B:Dut-C-cpm2#

```

lsp-ingress-stats

- Syntax** **lsp-ingress-stats** **lsp** *lsp-name* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]
- Context** monitor>router>mpls
- Description** This command displays ingress statistics for LSP interfaces at the configured interval until the configured count is reached.
- Default** N/A
- Parameters**
- repeat** *repeat* — specifies how many times the command is repeated
 - Values** 10
 - Values** 1 to 999
 - interval** *seconds* — specifies the interval for each display, in seconds
 - Values** 10
 - Values** 3 to 60
 - absolute** — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.
 - rate** — rate-per-second for each statistic is displayed instead of the delta
- Output**

Sample Output

```

B:Dut-C-cpm2# monitor router mpls lsp-ingress-stats lsp sample 1.1.1.1 repeat 3
interval 10 absolute
=====
Monitor ingress statistics for MPLS LSP "sample"
-----
At time t = 0 sec (Base Statistics)
-----
LSP Name      : sample
Sender       : 1.1.1.1
-----
Collect Stats : Enabled
Adm State     : Up
FC BE
InProf Pkts   : 539
InProf Octets : 548702
FC L2
Accting Plcy. : None
PSB Match     : True
OutProf Pkts  : 0
OutProf Octets: 0

```



```

InProf Pkts   : 0
InProf Octets : 0
FC AF
InProf Pkts   : 0
InProf Octets : 0
FC L1
InProf Pkts   : 1078
InProf Octets : 1097404
FC H2
InProf Pkts   : 0
InProf Octets : 0
FC EF
InProf Pkts   : 539
InProf Octets : 548702
FC H1
InProf Pkts   : 539
InProf Octets : 548702
FC NC
InProf Pkts   : 0
InProf Octets : 0
OutProf Pkts   : 539
OutProf Octets : 548702
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 539
OutProf Octets : 548702
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 539
OutProf Octets : 548702

```

At time t = 10 sec (Mode: Absolute)

LSP Name : sample
Sender : 1.1.1.1

```

Collect Stats : Enabled
Adm State     : Up
FC BE
InProf Pkts   : 568
InProf Octets : 578224
FC L2
InProf Pkts   : 0
InProf Octets : 0
FC AF
InProf Pkts   : 0
InProf Octets : 0
FC L1
InProf Pkts   : 1136
InProf Octets : 1156448
FC H2
InProf Pkts   : 0
InProf Octets : 0
FC EF
InProf Pkts   : 568
InProf Octets : 578224
FC H1
InProf Pkts   : 568
InProf Octets : 578224
FC NC
InProf Pkts   : 0
InProf Octets : 0
Accting Plcy. : None
PSB Match     : True
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 568
OutProf Octets : 578224
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 568
OutProf Octets : 578224
OutProf Pkts   : 0
OutProf Octets : 0
OutProf Pkts   : 568
OutProf Octets : 578224

```

At time t = 20 sec (Mode: Absolute)

LSP Name : sample
Sender : 1.1.1.1

Collect Stats : Enabled Accting Plcy. : None

```

Adm State      : Up                      PSB Match      : True
FC BE
InProf Pkts    : 597                     OutProf Pkts   : 0
InProf Octets  : 607746                  OutProf Octets : 0
FC L2
InProf Pkts    : 0                       OutProf Pkts   : 597
InProf Octets  : 0                       OutProf Octets : 607746
FC AF
InProf Pkts    : 0                       OutProf Pkts   : 0
InProf Octets  : 0                       OutProf Octets : 0
FC L1
InProf Pkts    : 1194                    OutProf Pkts   : 0
InProf Octets  : 1215492                 OutProf Octets : 0
FC H2
InProf Pkts    : 0                       OutProf Pkts   : 597
InProf Octets  : 0                       OutProf Octets : 607746
FC EF
InProf Pkts    : 597                     OutProf Pkts   : 0
InProf Octets  : 607746                  OutProf Octets : 0
FC H1
InProf Pkts    : 597                     OutProf Pkts   : 0
InProf Octets  : 607746                  OutProf Octets : 0
FC NC
InProf Pkts    : 0                       OutProf Pkts   : 597
InProf Octets  : 0                       OutProf Octets : 607746

```

At time t = 30 sec (Mode: Absolute)

```

LSP Name       : sample
Sender         : 1.1.1.1

```

```

Collect Stats  : Enabled                  Accting Plcy.  : None
Adm State      : Up                      PSB Match      : True
FC BE
InProf Pkts    : 627                     OutProf Pkts   : 0
InProf Octets  : 638286                  OutProf Octets : 0
FC L2
InProf Pkts    : 0                       OutProf Pkts   : 627
InProf Octets  : 0                       OutProf Octets : 638286
FC AF
InProf Pkts    : 0                       OutProf Pkts   : 0
InProf Octets  : 0                       OutProf Octets : 0
FC L1
InProf Pkts    : 1254                    OutProf Pkts   : 0
InProf Octets  : 1276572                 OutProf Octets : 0
FC H2
InProf Pkts    : 0                       OutProf Pkts   : 627
InProf Octets  : 0                       OutProf Octets : 638286
FC EF
InProf Pkts    : 627                     OutProf Pkts   : 0
InProf Octets  : 638286                  OutProf Octets : 0
FC H1
InProf Pkts    : 627                     OutProf Pkts   : 0
InProf Octets  : 638286                  OutProf Octets : 0
FC NC
InProf Pkts    : 0                       OutProf Pkts   : 627
InProf Octets  : 0                       OutProf Octets : 638286

```

=====

B:Dut-C-cpm2#

ospf

Syntax	ospf [<i>ospf-instance</i>]
Context	monitor>router>ospf
Description	This command enables the context to configure monitor commands for the OSPF instance.
Default	N/A
Parameters	<i>ospf-instance</i> — specifies the OSPF instance
	Values 1 to 31

ospf3

Syntax	ospf3
Context	monitor>router
Description	This command enables the context to configure monitor commands for the OSPF3 instance.
Default	N/A

interface

Syntax	interface <i>interface</i> [<i>interface...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>ospf monitor>router>ospf3
Description	<p>This command displays statistics for OSPF interfaces at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the OSPF interface(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A

Parameters *interface* — specifies the IP address of the interface (*ip-address*) or interface name (*ip-int-name*). Up to 5 interfaces can be specified. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

interval *seconds* — configures the interval for each display in seconds

Default 5 seconds

Values 3 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12>monitor>router>ospf# interface to-104 interval 3 repeat 3 absolute
=====
Monitor statistics for OSPF Interface "to-104"
=====
At time t = 0 sec (Base Statistics)
-----
Tot Rx Packets : 8379          Tot Tx Packets : 8528
Rx Hellos      : 8225          Tx Hellos      : 8368
Rx DBDs        : 6             Tx DBDs        : 12
Rx LSRs        : 2             Tx LSRs        : 1
Rx LSUs        : 55            Tx LSUs        : 95
Rx LS Acks     : 91            Tx LS Acks     : 52
Retransmits    : 2             Discards       : 0
Bad Networks   : 0             Bad Virt Links : 0
Bad Areas      : 0             Bad Dest Addrs : 0
Bad Auth Types : 0             Auth Failures  : 0
Bad Neighbors  : 0             Bad Pkt Types  : 0
Bad Lengths    : 0             Bad Hello Int. : 0
Bad Dead Int.  : 0             Bad Options    : 0
Bad Versions   : 0
-----
At time t = 3 sec (Mode: Absolute)
-----
Tot Rx Packets : 8379          Tot Tx Packets : 8528
Rx Hellos      : 8225          Tx Hellos      : 8368
Rx DBDs        : 6             Tx DBDs        : 12
Rx LSRs        : 2             Tx LSRs        : 1
Rx LSUs        : 55            Tx LSUs        : 95
Rx LS Acks     : 91            Tx LS Acks     : 52
Retransmits    : 2             Discards       : 0
Bad Networks   : 0             Bad Virt Links : 0
Bad Areas      : 0             Bad Dest Addrs : 0
Bad Auth Types : 0             Auth Failures  : 0
```

```

Bad Neighbors : 0
Bad Lengths   : 0
Bad Dead Int. : 0
Bad Versions  : 0
Bad Pkt Types : 0
Bad Hello Int.: 0
Bad Options   : 0

```

At time t = 6 sec (Mode: Absolute)

```

Tot Rx Packets : 8380
Rx Hellos      : 8226
Rx DBDs        : 6
Rx LSRs        : 2
Rx LSUs        : 55
Rx LS Acks     : 91
Retransmits    : 2
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Bad Lengths    : 0
Bad Dead Int.  : 0
Bad Versions   : 0
Tot Tx Packets : 8529
Tx Hellos      : 8369
Tx DBDs        : 12
Tx LSRs        : 1
Tx LSUs        : 95
Tx LS Acks     : 52
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0
Bad Hello Int. : 0
Bad Options    : 0

```

At time t = 9 sec (Mode: Absolute)

```

Tot Rx Packets : 8380
Rx Hellos      : 8226
Rx DBDs        : 6
Rx LSRs        : 2
Rx LSUs        : 55
Rx LS Acks     : 91
Retransmits    : 2
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Bad Lengths    : 0
Bad Dead Int.  : 0
Bad Versions   : 0
Tot Tx Packets : 8529
Tx Hellos      : 8369
Tx DBDs        : 12
Tx LSRs        : 1
Tx LSUs        : 95
Tx LS Acks     : 52
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0
Bad Hello Int. : 0
Bad Options    : 0

```

=====

```

A:ALA-12>monitor>router>ospf#

```

```

A:ALA-12>monitor>router>ospf# interface to-104 interval 3 repeat 3 rate

```

=====

```

Monitor statistics for OSPF Interface "to-104"
=====

```

At time t = 0 sec (Base Statistics)

```

Tot Rx Packets : 8381
Rx Hellos      : 8227
Rx DBDs        : 6
Rx LSRs        : 2
Rx LSUs        : 55
Rx LS Acks     : 91
Retransmits    : 2
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Tot Tx Packets : 8530
Tx Hellos      : 8370
Tx DBDs        : 12
Tx LSRs        : 1
Tx LSUs        : 95
Tx LS Acks     : 52
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0

```

```

Bad Lengths      : 0
Bad Dead Int.    : 0
Bad Versions     : 0
Bad Hello Int.   : 0
Bad Options      : 0

```

```
-----
At time t = 3 sec (Mode: Rate)
-----
```

```

Tot Rx Packets : 0
Rx Hellos      : 0
Rx DBDs        : 0
Rx LSRs        : 0
Rx LSUs        : 0
Rx LS Acks     : 0
Retransmits    : 0
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Bad Lengths    : 0
Bad Dead Int.  : 0
Bad Versions   : 0

Tot Tx Packets : 0
Tx Hellos      : 0
Tx DBDs        : 0
Tx LSRs        : 0
Tx LSUs        : 0
Tx LS Acks     : 0
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0
Bad Hello Int. : 0
Bad Options    : 0

```

```
-----
At time t = 6 sec (Mode: Rate)
-----
```

```

Tot Rx Packets : 0
Rx Hellos      : 0
Rx DBDs        : 0
Rx LSRs        : 0
Rx LSUs        : 0
Rx LS Acks     : 0
Retransmits    : 0
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Bad Lengths    : 0
Bad Dead Int.  : 0
Bad Versions   : 0

Tot Tx Packets : 0
Tx Hellos      : 0
Tx DBDs        : 0
Tx LSRs        : 0
Tx LSUs        : 0
Tx LS Acks     : 0
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0
Bad Hello Int. : 0
Bad Options    : 0

```

```
-----
At time t = 9 sec (Mode: Rate)
-----
```

```

Tot Rx Packets : 0
Rx Hellos      : 0
Rx DBDs        : 0
Rx LSRs        : 0
Rx LSUs        : 0
Rx LS Acks     : 0
Retransmits    : 0
Bad Networks   : 0
Bad Areas      : 0
Bad Auth Types : 0
Bad Neighbors  : 0
Bad Lengths    : 0
Bad Dead Int.  : 0
Bad Versions   : 0

Tot Tx Packets : 0
Tx Hellos      : 0
Tx DBDs        : 0
Tx LSRs        : 0
Tx LSUs        : 0
Tx LS Acks     : 0
Discards       : 0
Bad Virt Links : 0
Bad Dest Adrs  : 0
Auth Failures  : 0
Bad Pkt Types  : 0
Bad Hello Int. : 0
Bad Options    : 0

```

```
=====
A:ALA-12>monitor>router>ospf#
```

neighbor

Syntax	neighbor <i>ip-address</i> [<i>ip-address...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]								
Context	monitor>router>ospf monitor>router>ospf3								
Description	<p>This command displays statistical OSPF or OSPF3 neighbor information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified OSPF neighbor(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>								
Default	N/A								
Parameters	<p>neighbor <i>ip-address</i> — the IP address to display information for entries received from the specified OPSF neighbor. Up to 5 IP addresses can be specified.</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <table> <tr> <td>Default</td><td>5 seconds</td></tr> <tr> <td>Values</td><td>3 to 60</td></tr> </table> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <table> <tr> <td>Default</td><td>10</td></tr> <tr> <td>Values</td><td>1 to 999</td></tr> </table> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>	Default	5 seconds	Values	3 to 60	Default	10	Values	1 to 999
Default	5 seconds								
Values	3 to 60								
Default	10								
Values	1 to 999								

Output

Sample Output

```
A:ALA-12>monitor>router# ospf neighbor 10.0.0.104 interval 3 repeat 3 absolute
=====
Monitor statistics for OSPF Neighbor 10.0.0.104
=====
At time t = 0 sec (Base Statistics)
-----
Bad Nbr States      : 0                LSA Inst fails    : 0
Bad Seq Nums        : 0                Bad MTUs          : 0
```

```

Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 3 sec (Mode: Absolute)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 6 sec (Mode: Absolute)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 9 sec (Mode: Absolute)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
=====
A:ALA-12>monitor>router#

A:ALA-12>monitor>router# ospf neighbor 10.0.0.104 interval 3 repeat 3 absolute
=====
Monitor statistics for OSPF Neighbor 10.0.0.104
=====
-----
At time t = 0 sec (Base Statistics)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 3 sec (Mode: Rate)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 6 sec (Mode: Rate)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0
-----
At time t = 9 sec (Mode: Rate)
-----
Bad Nbr States   : 0          LSA Inst fails  : 0
Bad Seq Nums     : 0          Bad MTUs        : 0
Bad Packets      : 0          LSA not in LSDB : 0
Option Mismatches: 0          Nbr Duplicates  : 0

```



```
=====
A:ALA-12>monitor>router#
```

neighbor

Syntax	neighbor [<i>router-id</i>] [<i>interface-name</i>] [<i>interval seconds</i>] [repeat <i>repeat</i>] [absolute rate]								
Context	monitor>router>ospf monitor>router>ospf3								
Description	<p>This command displays statistical OSPF or OSPF3 neighbor information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified OSPF neighbor(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>								
Default	N/A								
Parameters	<p>neighbor <i>ip-address</i> — the IP address to display information for entries received from the specified OSPF neighbor. Up to 5 IP addresses can be specified.</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <table> <tr> <td>Default</td><td>5 seconds</td></tr> <tr> <td>Values</td><td>3 to 60</td></tr> </table> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <table> <tr> <td>Default</td><td>10</td></tr> <tr> <td>Values</td><td>1 to 999</td></tr> </table> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p> <p><i>router-id</i> — the router ID for an existing IP interface</p>	Default	5 seconds	Values	3 to 60	Default	10	Values	1 to 999
Default	5 seconds								
Values	3 to 60								
Default	10								
Values	1 to 999								

virtual-link

Syntax	virtual-link <i>nbr-rtr-id</i> area <i>area-id</i> [<i>interval seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>ospf

	monitor>router>ospf3
Description	<p>This command displays statistical OSPF virtual link information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified neighbor(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p> <p>When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p><i>nbr-rtr-id</i> — the IP address to uniquely identify a neighboring router in the autonomous system</p> <p><i>area area-id</i> — the OSPF area ID, expressed in dotted decimal notation or as a 32-bit decimal integer</p> <p>interval seconds — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat repeat — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

virtual-neighbor

Syntax	virtual-neighbor <i>nbr-rtr-id area area-id</i> [interval seconds] [repeat repeat] [absolute rate]
Context	monitor>router>ospf monitor>router>ospf3
Description	<p>This command displays statistical OSPF virtual neighbor information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified OSPF virtual neighbor router. The subsequent statistical information listed for each interval is displayed as a delta to the previous display.</p>

When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

Default	N/A
Parameters	<p><i>nbr-rtr-id</i> — the IP address to uniquely identify a neighboring router in the autonomous system</p> <p><i>area area-id</i> — the OSPF area ID, expressed in dotted decimal notation or as a 32-bit decimal integer</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

group

Syntax	group <i>grp-ip-address</i> [source <i>ip-address</i>] [interval <i>interval</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>pim
Description	This command monitors statistics for a PIM source group.
Default	N/A
Parameters	<p><i>grp-ip-address</i> — the IP address of an multicast group that identifies a set of recipients that are interested in a particular data stream</p> <p>source <i>ip-address</i> — the source IP address to use in the ping requests in dotted decimal notation</p> <p>Default the IP address of the egress IP interface</p> <p>Values 0.0.0.0 to 255.255.255.255</p> <p>interval <i>interval</i> — configures the interval for each display in seconds</p> <p>Default 10 seconds</p> <p>Values 10, 20, 30, 40, 50, 60</p>

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — rate-per-second for each statistic is displayed instead of the delta

neighbor

Syntax	neighbor <i>neighbor</i> [<i>neighbor...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>rip
Description	<p>This command displays statistical RIP neighbor information at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the specified RIP neighbor(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p>neighbor <i>ip-address</i> — the IP address to display information for entries received from the specified RIP neighbor. Up to 5 IP addresses can be displayed.</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 5 seconds</p> <p>Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

interface

Syntax	interface <i>interface</i> [<i>interface...</i> (up to 5 max)] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>router>rsvp
Description	<p>This command displays statistics for RSVP interfaces at the configured interval until the configured count is reached.</p> <p>The first screen displays the current statistics related to the RSVP interface(s). The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword rate is specified, the rate-per-second for each statistic is displayed instead of the delta.</p> <p>Monitor commands are similar to show commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.</p>
Default	N/A
Parameters	<p><i>interface</i> — specifies the IP address of the interface (<i>ip-address</i>) or interface name (<i>ip-int-name</i>). Up to 5 interfaces can be specified. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p style="padding-left: 40px;">Default 5 seconds</p> <p style="padding-left: 40px;">Values 3 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p style="padding-left: 40px;">Default 10</p> <p style="padding-left: 40px;">Values 1 to 999</p> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>

vrrp

Syntax	vrrp
Context	monitor>router
Description	This command enables the context to configure criteria to monitor VRRP statistical information for a VRRP enabled on a specific interface.
Default	N/A

instance

Syntax	instance interface <i>interface-name</i> vr-id <i>virtual-router-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]								
Context	monitor>router>vrrp								
Description	This command monitors statistics for a VRRP instance.								
Default	N/A								
Parameters	<p><i>interface-name</i> — the name of the existing IP interface on which VRRP is configured</p> <p>vr-id <i>virtual-router-id</i> — the virtual router ID for the existing IP interface, expressed as a decimal integer</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <table><tr><td>Default</td><td>5 seconds</td></tr><tr><td>Values</td><td>3 to 60</td></tr></table> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <table><tr><td>Default</td><td>10</td></tr><tr><td>Values</td><td>1 to 999</td></tr></table> <p>absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — rate-per-second for each statistic is displayed instead of the delta</p>	Default	5 seconds	Values	3 to 60	Default	10	Values	1 to 999
Default	5 seconds								
Values	3 to 60								
Default	10								
Values	1 to 999								

service

Syntax	service
Context	monitor
Description	This command enables the context to configure criteria to monitor specific service SAP criteria.
Default	N/A

id

Syntax	id <i>service-id</i>
Context	monitor>service
Description	This command displays statistics for a specific service, specified by the <i>service-id</i> , at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the *service-id*. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

Default	N/A
Parameters	<i>service-id</i> — the unique service identification number which identifies the service in the service domain

sap

Syntax	sap <i>sap-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>service>id
Description	This command monitors statistics for a SAP associated with this service.

This command displays statistics for a specific SAP, identified by the *port-id* and encapsulation value, at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the SAP. The subsequent statistical information listed for each interval is displayed as a delta to the previous display. When the keyword **rate** is specified, the rate-per-second for each statistic is displayed instead of the delta.

Monitor commands are similar to **show** commands but only statistical information displays. Monitor commands display the selected statistics according to the configured number of times at the interval specified.

Default	N/A
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition

Values

:null	<i>port-id</i> <i>bundle-id</i> <i>bpgrp-id</i> <i>lag-id</i> <i>aps-id</i>
dot1q	<i>port-id</i> <i>bundle-id</i> <i>bpgrp-id</i> <i>lag-id</i> <i>aps-id</i> <i>pw-id</i> : <i>[qtag1 cp-conn-prof-id]</i>
qinq	<i>port-id</i> <i>bundle-id</i> <i>bpgrp-id</i> <i>lag-id</i> <i>pw-id</i> : <i>[qtag1 cp-conn-prof-id].[qtag2 cp-conn-prof-id]</i>
	cp keyword
	<i>conn-prof-id</i> 1 to 8000
atm	<i>port-id</i> <i>aps-id</i> [: <i>vpi/vci</i> <i>vpi</i> <i>vpi1.vpi2</i> cp . <i>conn-prof-id</i>]

	cp	keyword
	<i>conn-prof-id</i>	1 to 8000
frame	<i>port-id aps-id:dlci</i>	
cisco-hdlc	<i>slot/mda/port.channel</i>	
cem	<i>slot/mda/port.channel</i>	
ima-grp	bundle-id [:vpi/vci vpi vpi1.vpi2 cp.conn-prof-id]	
	cp	keyword
	<i>conn-prof-id</i>	1 to 8000
port-id	<i>slot/mda/port[.channel]</i>	
	esat-id/slot/port	
	pxc-id.sub-port	
bundle-id	bundle-type-slot/mda.-bundle-num	
	bundle	keyword
	<i>type</i>	ima fr ppp
	<i>bundle-num</i>	1 to 336
bpgrp-id	bpgrp-type-bpgrp-num	
	bgrp	keyword
	<i>type</i>	ima ppp
	<i>bgrp-num</i>	1 to 2000
aps-id	aps-group-id[.channel]	
	aps	keyword
	<i>group-id</i>	1 to 128
ccag-id	ccag-id.path-id[cc-type]:cc-id	
	ccag	keyword
	<i>id</i>	1 to 8
	<i>path-id</i>	a b
	<i>cc-type</i>	.sap-net .net-sap
	<i>cc-id</i>	1 to 4094
eth-tunnel	eth-tunnel-id[:eth-tun-sap-id]	
	<i>id</i>	1 to 1024
	<i>eth-tun-sap-id</i>	0 to 4094
lag-id	lag-id	
	lag	keyword
	<i>id</i>	1 to 800
pw-id	pw-id	
	pw	keyword
	<i>id</i>	1 to 10239
qtag1	* 0 to 4094	
qtag2	* null 0 to 4094	

	<i>id</i>	1 to 8
	<i>path-id</i>	a b
	<i>cc-type</i>	.sap-net .net-sap
	<i>cc-id</i>	1 to 4094
eth-tunnel	eth-tunnel- <i>id</i> [: <i>eth-tun-sap-id</i>]	
	<i>id</i>	1 to 1024
	<i>eth-tun-sap-id</i>	0 to 4094
lag-id	lag-id	
	lag	keyword
	<i>id</i>	1 to 800
pw-id	pw-id	
	pw	keyword
	<i>id</i>	1 to 10239
qtag1	* 0 to 4094	
qtag2	* null 0 to 4094	

port-id — specifies the physical port ID in the *slot/mda/port*, **esat-id/slot/port** or **pxc-id.sub-port** format

If the card in the slot has XMA/MDAs installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 6/2/3 specifies port 3 on XMA/MDA 2 in slot 6.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels, the port ID must include the channel ID. A period “.” separates the physical port from the *channel-id*. The port must be configured as an access port. Channels are supported on the 7750 SR.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

bundle-id — specifies the multilink bundle to be associated with this IP interface. The **bundle** keyword must be entered at the beginning of the parameter. This parameter applies to the 7750 SR.

The command syntax must be configured as follows:

bundle-id: **bundle**-type-slot-id/mda-slot.bundle-num

bundle-id value range: 1 to 128

For example:

```
*A:ALA-12>config# port bundle-ppp-5/1.1
*A:ALA-12>config>port# multilink-bundle
```

bpgrp-id — specifies the bundle protection group ID to be associated with this IP interface. The **bpgrp** keyword must be entered at the beginning of the parameter. This parameter applies to the 7750 SR.

The command syntax must be configured as follows:

```
bpgrp-id:                bpgrp-type-bpgrp-num
type:                    ima
bpgrp-num value range:   1 to 1280
```

Example:

```
*A:ALA-12>config# port bpgrp-ima-1
*A:ALA-12>config>service>vpls$ sap bpgrp-ima-1
```

qtag1, *qtag2* — specifies the encapsulation value used to identify the SAP on the port or sub-port. If this parameter is not specifically defined, the default value is 0.

Values

```
qtag1:                    0 to 4094
qtag2 :                   * | 0 to 4094
```

The values depends on the encapsulation type configured for the interface. The following table describes the allowed values for the port and encapsulation types:

Table 22 **qtag values by port and encapsulation type**

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	0	The SAP is identified by the port.
Ethernet	Dot1q	0 to 4094	The SAP is identified by the 802.1Q tag on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.
Ethernet	QinQ	qtag1: 0 to 4094 qtag2: 0 to 4094	The SAP is identified by two 802.1Q tags on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.
SONET/ SDH	IPCP	—	The SAP is identified by the channel. No BCP is deployed and all traffic is IP.

Table 22 qtag values by port and encapsulation type (Continued)

Port Type	Encap-Type	Allowed Values	Comments
SONET/ SDH TDM	BCP-Null	0	The SAP is identified with a single service on the channel. Tags are assumed to be part of the customer packet and not a service delimiter.
SONET/ SDH TDM	BCP-Dot1q	0 to 4094	The SAP is identified by the 802.1Q tag on the channel.
SONET/ SDH TDM	Frame Relay	16 to 991	The SAP is identified by the data link connection identifier (DLCI).
SONET/ SDH ATM	ATM	vpi (NNI) 0 to 4095 vpi (UNI) 0 to 255 vci 1, 2, 5 to 65535	The SAP is identified by port or by PVPC or PVCC identifier (vpi, vpi/vci, or vpi range)

interval *seconds* — configures the interval for each display in seconds

Default 11 seconds

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — absolute rate-per-second value for each statistic is displayed

rate — rate-per-second for each statistic is displayed instead of the delta.

Output

Sample Output

```
*A:cses-A13# monitor service id 88 sap 1/1/2:0
=====
Monitor statistics for Service 88 SAP 1/1/2:0
=====
-----
At time t = 0 sec (Base Statistics)
-----
-----
Sap Statistics
-----
Last Cleared Time      : N/A
                        Packets
Forwarding Engine Stats                               Octets
```

Dropped	: 0	0
Off. HiPrio	: 0	0
Off. LowPrio	: 0	0
Off. Uncolor	: 0	0
Queueing Stats(Ingress QoS Policy 1)		
Dro. HiPrio	: 0	0
Dro. LowPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0
Queueing Stats(Egress QoS Policy 1)		
Dro. InProf	: 0	0
Dro. OutProf	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

Sap per Queue Stats		

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LoPrio	: 0	0
Dro. HiPrio	: 0	0
Dro. LoPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

sdp

Syntax	sdp { <i>sdp-id</i> far-end <i>ip-address</i> } [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>service>id
Description	This command monitors statistics for a SDP binding associated with this service.
Default	N/A
Parameters	<p><i>sdp-id</i> — specifies the SDP identifier</p> <p>Values 1 to 17407</p> <p>far-end <i>ip-address</i> — the system address of the far-end router for the SDP in dotted decimal notation</p> <p>interval <i>seconds</i> — configures the interval for each display in seconds</p> <p>Default 11 seconds</p> <p>Values 11 to 60</p> <p>repeat <i>repeat</i> — configures how many times the command is repeated</p> <p>Default 10</p> <p>Values 1 to 999</p>

absolute — absolute rate-per-second value for each statistic is displayed

rate — rate-per-second for each statistic is displayed instead of the delta

Output

Sample Output

```
A:ALA-12# monitor service id 100 sdp 10 repeat 3
=====
Monitor statistics for Service 100 SDP binding 10
=====
At time t = 0 sec (Base Statistics)
-----
I. Fwd. Pkts.   : 0                      I. Dro. Pkts.   : 0
E. Fwd. Pkts.   : 0                      E. Fwd. Octets  : 0
-----
At time t = 11 sec (Mode: Delta)
-----
I. Fwd. Pkts.   : 0                      I. Dro. Pkts.   : 0
E. Fwd. Pkts.   : 0                      E. Fwd. Octets  : 0
-----
At time t = 22 sec (Mode: Delta)
-----
I. Fwd. Pkts.   : 0                      I. Dro. Pkts.   : 0
E. Fwd. Pkts.   : 0                      E. Fwd. Octets  : 0
-----
At time t = 33 sec (Mode: Delta)
-----
I. Fwd. Pkts.   : 0                      I. Dro. Pkts.   : 0
E. Fwd. Pkts.   : 0                      E. Fwd. Octets  : 0
=====
A:ALA-12#
```

subscriber

Syntax	subscriber <i>sub-ident-string</i> sap <i>sap-id</i> sla-profile <i>sla-profile-name</i> [base ingress-queue-id <i>ingress-queue-id</i> egress-queue-id <i>egress-queue-id</i>] [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor>service
Description	This command monitors statistics for a subscriber.
Parameters	sub-ident-string — specifies an existing subscriber identification profile to monitor sap <i>sap-id</i> — specifies the physical port identifier portion of the SAP definition Values dpci 16 to 1022 sla-profile <i>sla-profile-name</i> — specifies an existing SLA profile

interval *seconds* — configures the interval for each display in seconds

Default 11

Values 11 to 60

repeat *repeat* — configures how many times the command is repeated

Default 10

Values 1 to 999

absolute — raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

Default mode delta

rate — rate-per-second for each statistic is displayed instead of the delta

base — monitor base statistics

ingress-queue-id *ingress-queue-id* — monitors statistics for this queue

Values 1 to 32

egress-queue-id *egress-queue-id* — monitors statistics for this queue

Values 1 to 8

Output

Sample Output

```
A:Dut-A# monitor service subscriber nokia_100 sap 1/2/1:101 sla-profile sla_
default
=====
Monitor statistics for Subscriber nokia_100
=====
At time t = 0 sec (Base Statistics)
-----
SLA Profile Instance statistics
-----

```

	Packets	Octets
Off. HiPrio	: 0	0
Off. LowPrio	: 94531	30704535
Off. Uncolor	: 0	0

```

Queueing Stats (Ingress QoS Policy 1000)
Dro. HiPrio      : 0                      0
Dro. LowPrio     : 7332                   2510859
For. InProf      : 0                      0
For. OutProf     : 87067                  28152288

Queueing Stats (Egress QoS Policy 1000)
Dro. InProf      : 880                    127660
Dro. OutProf     : 0                      0
For. InProf      : 90862                  12995616
For. OutProf     : 0                      0
-----
SLA Profile Instance per Queue statistics

```

```

-----
                Packets                Octets
Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio      : 0                    0
Off. LowPrio     : 0                    0
Off. Uncolor     : 0                    0
Dro. HiPrio      : 0                    0
Dro. LowPrio     : 0                    0
For. InProf      : 0                    0
For. OutProf     : 0                    0

Ingress Queue 2 (Unicast) (Priority)
Off. HiPrio      : 0                    0
Off. LowPrio     : 94531                30704535
Off. Uncolor     : 0                    0
Dro. HiPrio      : 0                    0
Dro. LowPrio     : 7332                 2510859
For. InProf      : 0                    0
For. OutProf     : 87067                28152288

Ingress Queue 3 (Unicast) (Priority)
Off. HiPrio      : 0                    0
Off. LowPrio     : 0                    0
Off. Uncolor     : 0                    0
Dro. HiPrio      : 0                    0
Dro. LowPrio     : 0                    0
For. InProf      : 0                    0
For. OutProf     : 0                    0

Ingress Queue 11 (Multipoint) (Priority)
Off. HiPrio      : 0                    0
Off. LowPrio     : 0                    0
Off. Uncolor     : 0                    0
Dro. HiPrio      : 0                    0
Dro. LowPrio     : 0                    0
For. InProf      : 0                    0
For. OutProf     : 0                    0

Egress Queue 1
Dro. InProf      : 880                  127660
Dro. OutProf     : 0                    0
For. InProf      : 90862                12995616
For. OutProf     : 0                    0

Egress Queue 2
Dro. InProf      : 0                    0
Dro. OutProf     : 0                    0
For. InProf      : 0                    0
For. OutProf     : 0                    0

Egress Queue 3
Dro. InProf      : 0                    0
Dro. OutProf     : 0                    0
For. InProf      : 0                    0
For. OutProf     : 0                    0
=====
A:Dut-A#

```

```

A:Dut-A# monitor service subscriber nokia_100 sap 1/2/1:101 sla-
profile sla_default base rate
=====
Monitor statistics for Subscriber nokia_100
=====
At time t = 0 sec (Base Statistics)
-----
SLA Profile Instance statistics
-----

```

	Packets	Octets
Off. HiPrio	: 0	0
Off. LowPrio	: 109099	35427060
Off. Uncolor	: 0	0
Queueing Stats (Ingress QoS Policy 1000)		
Dro. HiPrio	: 0	0
Dro. LowPrio	: 8449	2894798
For. InProf	: 0	0
For. OutProf	: 100523	32489663
Queueing Stats (Egress QoS Policy 1000)		
Dro. InProf	: 880	127660
Dro. OutProf	: 0	0
For. InProf	: 105578	15104553
For. OutProf	: 0	0

```

-----
At time t = 11 sec (Mode: Rate)
-----
SLA Profile Instance statistics
-----

```

	Packets	Octets	% Port Util.
Off. HiPrio	: 0	0	0.00
Off. LowPrio	: 1469	477795	0.38
Off. Uncolor	: 0	0	0.00
Queueing Stats (Ingress QoS Policy 1000)			
Dro. HiPrio	: 0	0	0.00
Dro. LowPrio	: 119	40691	0.03
For. InProf	: 0	0	0.00
For. OutProf	: 1349	437350	0.34
Queueing Stats (Egress QoS Policy 1000)			
Dro. InProf	: 0	0	0.00
Dro. OutProf	: 0	0	0.00
For. InProf	: 1469	209129	0.16
For. OutProf	: 0	0	0.00

```

=====
A:Dut-A#

A:Dut-A# monitor service subscriber nokia_100 sap 1/2/1:101 sla-
profile sla_default ingress-queue-id 1
=====
Monitor statistics for Subscriber nokia_100
=====
At time t = 0 sec (Base Statistics)
-----

```

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LowPrio	: 0	0


```
Off. Uncolor      : 0          0
Dro. HiPrio       : 0          0
Dro. LowPrio      : 0          0
For. InProf       : 0          0
For. OutProf      : 0          0
=====
A:Dut-A#

A:Dut-A# monitor service subscriber nokia_100 sap 1/2/1:101 sla-profile
sla_default egress-queue-id 1
=====
Monitor statistics for Subscriber nokia_100
-----
At time t = 0 sec (Base Statistics)
-----

```

	Packets	Octets
Egress Queue 1		
Dro. InProf	: 880	127660
Dro. OutProf	: 0	0
For. InProf	: 164366	23506178
For. OutProf	: 0	0

```
=====
A:Dut-A#
```

2.13.2.3 CLI Environment Commands

alias

Syntax	alias <i>alias-name alias-command-line</i> no alias <i>alias-name</i>
Context	environment
Description	This command enables the substitution of a command line (or part of a command line) by an alias. Use the alias command to create alternative or easier to remember/understand names for an entity or command string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. The special characters "/" and "\" cannot be used as the first character inside an alias string. An alias can contain a double quote character by preceding the quote with a "\" character (for example, alias my-alias " match \"string\""). Only a single command can be present in the command string (the command can be long with many parameters but there is no support for aliases that include multiple CLI commands/lines). 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 OSPF interfaces, enter:

alias soi "show router ospf interface"

Complex aliases can be created to have shortcuts for customized show routine output:

```
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"
```

and then used like this:

```
show port detail my-summary
```

Default N/A

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

alias-command-line — 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** — the **create** keyword is required

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 will be displayed, which may scroll the screen.

Default **more** — CLI output pauses at the end of each screen waiting for the user input to continue.

reduced-prompt

Syntax	reduced-prompt [number of nodes in prompt] no reduced-prompt				
Context	environment				
Description	<p>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, causing the CLI prompt to become too long. By default, the CLI prompt displays the system name and the complete context in the CLI.</p> <p>The number of <i>nodes</i> 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 an ellipsis ("...").</p> <pre>A:ALA-1>environment# reduced-prompt 2 A:ALA-1>vonfig>router# interface to-103 A:ALA-1>...router>if#</pre> <p>The setting is not saved in the configuration. It must be reset for each CLI session or stored in an exec script file.</p> <p>The no form of the command reverts to the default.</p>				
Default	no reduced-prompt — displays all context nodes in the CLI prompt				
Parameters	<p><i>number of nodes in prompt</i> — the maximum number of higher-level nodes displayed by name in the prompt, expressed as a decimal integer</p> <table><tr><td>Default</td><td>2</td></tr><tr><td>Values</td><td>0 to 15</td></tr></table>	Default	2	Values	0 to 15
Default	2				
Values	0 to 15				

saved-ind-prompt

Syntax	[no] saved-ind-prompt
Context	environment
Description	<p>This command enables 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.</p> <pre>*A:ALA-48# admin save Writing file to ftp://128.251.10.43/./sim48/sim48-config.cfg Saving configuration Completed. A:ALA-48#</pre>
Default	N/A

suggest-internal-objects

Syntax	[no] suggest-internal-objects
Context	environment
Description	This command enables suggesting of internally created objects while auto completing. The no form of the command disables the command.
Default	N/A

terminal

Syntax	terminal no terminal
Context	environment
Description	This command enables the context to configure the terminal screen length for the current CLI session.
Default	N/A

length

Syntax	length <i>lines</i>
Context	environment>terminal
Description	This command sets the number of lines on a screen.
Default	N/A
Parameters	<i>lines</i> — the number of lines for the terminal screen length, expressed as a decimal integer
Values	1 to 512
Default	24 — terminal dimensions are set to 24 lines long by 80 characters wide

width

Syntax	width <i>width</i>
Context	environment>terminal

Description	This command determines display terminal width.
Default	width 80 — terminal dimensions are set to 24 lines long by 80 characters wide
Parameters	<i>width</i> — sets the width of the display terminal
Values	1 to 512

time-display

Syntax	time-display {local utc}
Context	environment
Description	<p>This command displays time stamps in the CLI session based on local time or Coordinated Universal Time (UTC).</p> <p>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.</p> <p>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 time stamp is displayed.</p> <p>In general all time stamps 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.</p>
Default	time-display local — displays time stamps based on the local time

2.13.2.4 Candidate Commands

candidate

Syntax	candidate
Context	<root>
Description	<p>This command enables the context to edit candidate configurations.</p> <p>Commands in the candidate CLI branch, except candidate edit, are available only when in edit-cfg mode.</p>
Default	N/A

edit

Syntax	edit [exclusive]
Context	candidate
Description	This command enables the edit-cfg mode where changes can be made to the candidate configuration and sets the edit-point to the end of the candidate. In edit-cfg mode the CLI prompt contains edit-cfg near the root of the prompt. Commands in the candidate CLI branch, except candidate edit , are available only when in edit-cfg mode.
Default	N/A
Parameters	exclusive — allows a user to exclusively create a candidate configuration by blocking other users (and other sessions of the same user) from entering edit-cfg mode. Exclusive edit-cfg mode can only be entered if the candidate configuration is empty and no user is in edit-cfg mode. Once a user is in exclusive edit-cfg mode no other users/sessions are allowed in edit-cfg mode. The user must either commit or discard the exclusive candidate before leaving exclusive edit-cfg mode. If the CLI session times out while a user is in exclusive edit-cfg mode then the contents of the candidate are discarded. The admin disconnect command can be used to force a user to disconnect (and to clear the contents of the candidate) if they have the candidate locked.

commit

Syntax	commit [confirmed <i>timeout</i>] [comment <i>comment</i>] commit no-checkpoint [confirmed <i>timeout</i>]
Context	candidate
Description	<p>This command applies the changes in the candidate configuration to the active running configuration. The candidate changes will take operational effect.</p> <p>If a commit operation is successful then all of the candidate changes will take operational effect and the candidate is cleared. If there is an error in the processing of the commit, or a 'commit confirmed' is not confirmed and an auto-revert occurs, then the router will return to a configuration state with none of the candidate changes applied. The operator can then continue editing the candidate and try a commit later.</p> <p>By default, the SR OS will automatically create a new rollback checkpoint after a commit operation. The rollback checkpoint will contain the new configuration changes made by the commit. An optional no-checkpoint keyword can be used to avoid the auto-creation of a rollback checkpoint after a commit.</p> <p>A commit operation is blocked if a rollback revert is currently being processed.</p>
Default	N/A

Parameters	<p>confirmed — specifies that the commit operation (if successful) should be automatically reverted (undone) at the end of the timeout period unless the operator issues the confirm command before the timeout period expires. A rollback checkpoint is created after the commit operation (if successful) and will remain available whether the commit is auto-reverted or not. The contents of the candidate will remain visible (candidate view) and changes to the candidate are blocked until the timeout is completed or the candidate confirm command is executed. If the timeout expires and an auto-revert occurs, then the original candidate config will be available in edit-cfg mode.</p> <p>Standard line-by-line non-transactional configuration commands (including via SNMP) are not blocked during the countdown period and any changes made to the configuration during the countdown period will be rolled back if the timeout expires. The confirmed option is useful when changes are being made that could impact management reachability to the router.</p> <p>A rollback revert is blocked during the countdown period until the commit has been confirmed.</p> <p><i>timeout</i> — the auto-revert timeout period in minutes</p> <p>Values 1 to 168</p> <p>no-checkpoint — used to avoid the automatic creation of a rollback checkpoint for a successful commit</p> <p>comment <i>comment</i> — adds a comment up to 255 characters in length to the automatic rollback checkpoint</p>
-------------------	---

confirm

Syntax	confirm
Context	candidate
Description	<p>This command is used to stop an automatic reversion to the previous configuration after the candidate commit confirmed command was used. If the confirm command is not executed before the commit confirmed timeout period expires then the previous commit changes will be undone and the previous candidate configuration will be available for editing and a subsequent commit.</p> <p>During the countdown the contents of the candidate will remain visible (candidate view) and changes to the candidate are blocked until the timeout is completed or the candidate confirm command is executed. Executing the confirm command clears the contents of the candidate and allows editing of the candidate.</p>
Default	N/A

copy

Syntax	copy [line]
Context	candidate
Description	This command copies the selected CLI node (which includes all sub-branches) into a temporary buffer that can be used for a subsequent insert. The contents of the temporary buffer are deleted when the operator exits the candidate edit mode.
Default	N/A
Parameters	line — indicates which line to copy
	Values
	line, offset, first, edit-point, last
	line — absolute line number
	offset — relative line number to the current edit point. Prefixed with '+' or '-'.
	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 node (which includes all sub-branches). The deleted lines are also copied into a temporary buffer that can be used for a subsequent insert.
Default	N/A
Parameters	line — indicates which line to delete
	Values
	line, offset, first, edit-point last
	line
	absolute line number
	offset
	relative line number to current edit point. Prefixed with '+' or '-'
	first
	keyword - first line
	edit-point
	keyword - current edit point
	last
	keyword - 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 the edit-cfg mode. Undo cannot be used to recover a candidate that has been discarded with candidate discard .
Default	N/A
Parameters	now — avoids a 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 edit-cfg mode.
Default	N/A
Parameters	line — indicates which line to change starting at the point indicated by the following options
	Values
	line, offset, first, edit-point last
	line absolute line number
	offset relative line number to current edit point. Prefixed with '+' or '-'
	first keyword - first line
	edit-point keyword - current edit point
	last keyword - last line that is not 'exit'

insert

Syntax	insert [line]
Context	candidate

Description	<p>This command inserts the contents of the temporary buffer (populated by a previous copy or delete command) into the candidate configuration. The contents are inserted by default after the current edit point. Optional parameters allow the insertion after some other point of the candidate. The contents of the temporary buffer are deleted when the operator exits candidate edit mode.</p> <p>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 lines to be inserted are supported at the context of the insertion point then the lines are simply inserted into the configuration. If the lines to be inserted are not supported at the context of the insertion point, then the context at the insertion point is first closed using multiple exit statements, the context of the lines to be inserted is built (added) into the candidate at the insertion point, then the lines themselves are added, the context of the inserted lines is closed using exit statements and finally the context from the original insertion point is built again leaving the context at the same point as it was before the insertion.</p>		
Default	N/A		
Parameters	line — indicates where to insert the line starting at the point indicated by the following options		
	Values		
	line, offset, first, edit-point last		
	line	absolute line number	
	offset	relative line number to current edit point. Prefixed with '+' or '-'	
	first	keyword - first line	
	edit-point	keyword - current edit point	
	last	keyword - last line that is not 'exit'	

load

Syntax	load file-url [overwrite insert append]
Context	candidate
Description	<p>This command loads a previously saved candidate configuration into the current candidate. The edit point will be set to the end of the loaded configuration lines. The candidate configuration cannot be modified while a load is in progress.</p>
Default	<p>If the candidate is empty then a load without any of the optional parameters (such as overwrite, etc) will simply load the file-url into the candidate. If the candidate is not empty then one of the options, such as overwrite, insert, etc., must be specified.</p>
Parameters	<p>file-url — the directory and filename to load</p> <p>overwrite — discards the contents of the current candidate and replace it with the contents of the file</p>

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 the edit-cfg mode. The contents of the current candidate will not be deleted and the operator can continue editing the candidate later.
Default	N/A

redo

Syntax	redo [<i>count</i>]				
Context	candidate				
Description	<p>This command reapplies the changes to the candidate that were removed using a previous undo. All undo/redo history is lost when the operator exits edit-cfg mode.</p> <p>A redo command is blocked if another user has made changes in the same CLI branches that would be impacted during the redo.</p>				
Default	N/A				
Parameters	<p>count — the number of previous changes to reapply</p> <table> <tr> <td>Values</td><td>1 to 50</td></tr> <tr> <td>Default</td><td>1</td></tr> </table>	Values	1 to 50	Default	1
Values	1 to 50				
Default	1				

replace

Syntax	replace [<i>line</i>]		
Context	candidate		
Description	This command displays the specified line (a single line only) and allows it to be changed.		
Default	N/A		
Parameters	<p>line — indicates which line to replace starting at the point indicated by the following options</p> <table> <tr> <td>Values</td><td></td></tr> </table>	Values	
Values			

line, offset, first, edit-point last		
line		absolute line number
offset		relative line number to current edit point. Prefixed with '+' or '-'
first		keyword - first line
edit-point		keyword - current edit point
last		keyword - last line that is not 'exit'

save

Syntax	save <i>file-url</i>
Context	candidate
Description	This command saves the current candidate to a file.
Default	N/A
Parameters	<i>file-url</i> — the directory and filename

undo

Syntax	undo [<i>count</i>]
Context	candidate
Description	<p>This command removes the most recent change(s) done to the candidate. The changes can be reapplied using the redo command. All undo/redo history is lost when the operator exists edit-cfg mode. Undo can not be used to recover a candidate that has been discarded with candidate discard.</p> <p>An undo command is blocked if another user has made changes in the same CLI branches that would be impacted during the undo.</p>
Default	N/A
Parameters	count — the number of previous changes to remove
	Values 1 to 50
	Default 1

view

Syntax	view [<i>line</i>]
---------------	-----------------------------

Context	candidate										
Description	This command displays the candidate configuration along with line numbers that can be used for editing the candidate configuration.										
Default	N/A										
Parameters	line — displays the candidate configuration starting at the point indicated by the following options (the display is not limited to the current CLI context/branch)										
	Values line, offset, first, edit-point last										
	<table> <tr> <td>line</td><td>absolute line number</td></tr> <tr> <td>offset</td><td>relative line number to current edit point. Prefixed with '+' or '-'</td></tr> <tr> <td>first</td><td>keyword - first line</td></tr> <tr> <td>edit-point</td><td>keyword - current edit point</td></tr> <tr> <td>last</td><td>keyword - last line that is not 'exit'</td></tr> </table>	line	absolute line number	offset	relative line number to current edit point. Prefixed with '+' or '-'	first	keyword - first line	edit-point	keyword - current edit point	last	keyword - last line that is not 'exit'
line	absolute line number										
offset	relative line number to current edit point. Prefixed with '+' or '-'										
first	keyword - first line										
edit-point	keyword - current edit point										
last	keyword - last line that is not 'exit'										

info operational

Syntax	info {operational}
Context	<root>
Description	In edit-cfg mode, the operational keyword is mandatory when using the info command.
Default	N/A

candidate

Syntax	candidate
Context	show>system
Description	This command shows candidate configuration information.
Default	N/A
Output	The following table describes the candidate output fields:

Table 23 **Candidate output fields**

Label	Description
Candidate configuration state	<ul style="list-style-type: none"> • empty — indicates there are no uncommitted changes in the candidate config • modified — indicates there are uncommitted changes in the candidate config • unconfirmed — indicates there are no uncommitted changes in the candidate config but the result of the last commit will be auto-reverted unless it is confirmed before the timeout expires
Num editors/viewers	the number of CLI sessions currently in edit-cfg mode
Candidate cfg exclusive locked	indicates if a user has exclusively locked the candidate using the candidate edit exclusive command
Last commit state	<ul style="list-style-type: none"> • none — indicates there have been no commits since the last reboot of the node • in-progress — indicates the system is currently committing the candidate config • success — indicates the last commit finished successfully • revert-pending — indicates the last commit finished successfully but has not been confirmed yet, and will be auto-reverted if it is not confirmed before the timeout expires • failed — indicates the last commit failed and has been undone • revert-in-progress — indicates the last commit finished successfully but was not confirmed in time and is currently being reverted • reverted — indicates the last commit finished successfully but was not confirmed in time and has been reverted • revert-failed — indicates the last commit finished successfully but was not confirmed in time and the system attempted to revert it but failed
Last commit time	the time at which the last commit attempt was started
Checkpoint created with last commit	indicates if a rollback checkpoint was created after the previous commit completed
Scheduled revert time	used to indicate the currently scheduled auto-revert time based on the confirmed option being used with a candidate commit
Last commit revert time	the time the commit was last reverted
Users in edit-cfg mode	lists all the user sessions that are currently in edit-cfg mode

Table 23 Candidate output fields (Continued)

Label	Description (Continued)
Type (from)	indicates the type of session (such as Console, Telnet, etc.) and also the source of the session (such as the source IP address of the remote host)

Sample Output

```
*A:bksim3107# show system candidate
=====
Candidate Config Information
=====
Candidate configuration state           : modified
Num editors/viewers                    : 0
Candidate cfg exclusive locked         : no
Last commit state                      : revert-failed
Last commit time                       : 10/23/2012 17:21:47
Checkpoint created with last commit    : yes
Scheduled revert time                  : N/A
Last commit revert time                 : 10/23/2012 17:22:47

=====
Users in edit-cfg mode
=====
Username      Type (from)
=====
admin         Console
Joris         Telnet (172.31.117.239)
=====
```

2.13.2.5 Rollback Commands

compare

Syntax	compare [<i>to source2</i>] compare <i>source1 to source2</i>
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 displays the differences between rollback checkpoints and the active operational configuration, with source1 as the base/first file to which source2 is compared.

A compare operation does not check authorization of each line of output. Permission to execute the compare operation from the admin branch of CLI (authorization for the **admin rollback compare** or **admin compare** command itself) should only be given to users who are allowed to view the entire configuration, similar to permissions for **admin display-config**.

Default The defaults for source1 and source2 are context aware and differ based on the branch in which the command is executed. In general, the default for source1 matches the context from which the command is issued.

- In the admin node: No defaults. source1 and source2 must be specified.
- In the admin>rollback node:
source1 default = active-cfg, source2 default = latest-rb
compare: equivalent to “compare active-cfg to latest-rb”
compare to source2: equivalent to “compare active-cfg to source2”
- In a config>xx node:
compare to source2: equivalent to “compare active-cfg to source2”

Parameters *source1, source2* — specifies comparison information

Values **active-cfg** — the currently operational configuration that is active in the node
latest-rb — the most recent rollback checkpoint (the checkpoint file at the configured rollback-location with “*.rb” as the suffix)
rescue — the rescue configuration (at the configured rescue-location)
checkpoint-id — an id from [1 to max] indicating a specific rollback checkpoint (where max is the highest checkpoint allowed/configured). A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with “*.rb.1” as the suffix, 2 for file “*.rb.2”, etc.

delete

Syntax **delete {latest-rb | checkpoint-id | rescue}**

Context admin>rollback

Description This command deletes a rollback checkpoint and causes the suffixes to be adjusted (decremented) for all checkpoints older that the one that was deleted (to close the hole in the list of checkpoint files and create room to create another checkpoint).

If **config redundancy rollback-sync** is enabled, a rollback delete will also delete the equivalent checkpoint on the standby CF and shuffle the suffixes on the standby CF.

It is not advised to manually delete a rollback checkpoint (for example, using a **file delete** command). If a rollback checkpoint file is manually deleted without using the **admin rollback delete** command then the suffixes of the checkpoint files are NOT shuffled, nor is the equivalent checkpoint file deleted from the standby CF. This manual deletion creates a hole in the checkpoint file list until enough new checkpoints have been created to roll the hole off the end of the list.

Default N/A

Parameters **latest-rb** — specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file)

checkpoint-id — an id from [1 to *max*] indicating a specific rollback checkpoint (where *max* is the highest checkpoint allowed/configured). A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback location) with *.rb.1 as the suffix, 2 for file *.rb.2, etc.

rescue — deletes the rescue checkpoint. No checkpoint suffix numbers are changed.

revert

Syntax **revert** {**latest-rb** | *checkpoint-id* | **rescue**} [**now**]

Context admin>rollback

Description This command initiates a configuration rollback revert operation that will return the configuration state of the node to a previously saved checkpoint. The rollback revert minimizes impacts to running services. There are no impacts in areas of configuration that did not change since the checkpoint. Configuration parameters that changed (or items on which changed configuration have dependencies) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas).

Default N/A

Parameters **latest-rb** — specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file)

checkpoint-id — indicates the configuration to return to (which rollback checkpoint file to use). Checkpoint-id of 1 corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint. Max is the highest rollback checkpoint supported or configured.

Values 1—*max*, where *max* is the number of configured checkpoints minus 1 (since, for example, the 10th checkpoint has an id of 9)

rescue — revert to the rescue checkpoint

now — forces a rollback revert without any interactive confirmations (assumes 'y' for any confirmations that would have occurred)

save

Syntax	save [comment <i>comment-string</i>] [rescue]
Context	admin>rollback
Description	<p>If the optional rescue keyword is not used, this command saves a rollback checkpoint at the location and with the filename specified by the rollback-location with a suffix of .rb. The previously saved checkpoints will have their suffixes incremented by one (.rb.1 becomes .rb.2, etc). If there are already as many checkpoint files as the maximum number supported, then the last checkpoint file is deleted.</p> <p>If the rescue keyword is used, then this command saves the current operational configuration as a rescue configuration at the location and with the filename specified by the rescue location. The filename will have the suffix .rc appended.</p>
Default	N/A
Parameters	<p><i>comment-string</i> — a comment of up to 255 characters in length that is associated with the checkpoint</p> <p><i>rescue</i> — saves the rescue checkpoint instead of a normal rollback checkpoint</p>

view

Syntax	view [latest-rb <i>checkpoint-id</i> rescue]
Context	admin>rollback
Description	This command displays the checkpoint.
Default	N/A
Parameters	<p>latest-rb — specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file)</p> <p><i>checkpoint-id</i> — indicates rollback checkpoint file to be viewed. Checkpoint-id of 1 corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint. Max is the highest rollback checkpoint supported or configured.</p> <p>Values 1 to <i>max</i></p> <p>rescue — view the rescue configuration</p>

view

Syntax	view { active-cfg rescue latest-rb <i>checkpoint-id</i> }
Context	<root>

Description	The context to configure administrative system viewing parameters. Only authorized users can execute the commands in the admin context.
Default	N/A
Parameters	<p>bootup-cfg — specifies the bootup configuration</p> <p>active-cfg — specifies current running configuration</p> <p>candidate-cfg — specifies candidate configuration</p> <p>latest-rb — specifies the latest configuration</p> <p><i>checkpoint-id</i> — specifies a specific checkpoint file configuration</p> <p>Values 1 to 9</p> <p>rescue — specifies a rescue checkpoint configuration</p>

rollback-location

Syntax	rollback-location <i>file-url</i> / <i>rollback filename</i>
Context	config>system>rollback
Description	The location and name of the rollback checkpoint files is configurable to be local (on compact flash) or remote. The <i>file-url</i> must not contain a suffix (just a path/directory + filename). The suffixes for rollback checkpoint files are ".rb", ".rb.1", ..., ".rb.9" and are automatically appended to rollback checkpoint files.
Default	no rollback-location. A valid rollback-location must be configured before a rollback save is executed.
Parameters	<p><i>file-url</i> — specifies the URL</p> <p>Values</p> <p><i>local-url</i> <i>remote-url</i></p> <p><i>local-url</i> [<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including flash-id directory length 99 chars max each</p> <p><i>remote-url</i> [{ftp://}login:pswd@ <i>remote-locn</i>]/[<i>file-path</i>] 255 chars max directory length 99 chars max each</p> <p><i>remote-locn</i> [<i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i>]</p> <p><i>ipv4-address</i> a.b.c.d</p> <p><i>ipv6-address</i> x:x:x:x:x:x:x[-<i>interface</i>] x:x:x:x:x:x:d.d.d.d[-<i>interface</i>] x - [0 to FFFF]H d - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses</p> <p><i>cflash-id</i> cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</p>

rollback-filename — specifies the rollback file name

Values suffixed with .rb, .rb.1 up to .9 during rollback checkpoint creation

rescue-location

Syntax	[no] rescue-location <i>file-url</i>
Context	config>system>rollback
Description	The location and filename of the rescue configuration is configurable to be local (on compact flash) or remote. The suffix .rc will be automatically appended to the filename when a rescue configuration file is saved. Trivial FTP (TFTP) is not supported for remote locations.
Default	no rescue location. A valid rescue location must be configured before a rescue configuration is saved.
Parameters	<i>file-url</i> — specifies the URL
	Values
	<i>local-url</i> <i>remote-url</i>
	<i>local-url</i> [<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including flash-id directory length 99 chars max each
	<i>remote-url</i> [{ftp://}login:pswd@ <i>remote-locn</i>]/[<i>file-path</i>] 255 chars max directory length 99 chars max each
	<i>remote-locn</i> [<i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i>]
	<i>ipv4-address</i> a.b.c.d
	<i>ipv6-address</i> x:x:x:x:x:x:x[- <i>interface</i>] x:x:x:x:x:x:d.d.d.d[- <i>interface</i>] x - [0 to FFFF]H d - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses
	<i>cflash-id</i> cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
	rescue filename suffixed with rc during rescue file creation

local-max-checkpoints

Syntax	local-max-checkpoints <i>local-max-checkpoints</i>
Context	config>system>rollback
Description	Configures the maximum number of rollback checkpoint files when the rollback-location is on local compact flash.

Default	local-max-checkpoints 10
Parameters	<i>local-max-checkpoints</i> — 1 to 50

remote-max-checkpoints

Syntax	remote-max-checkpoints <i>remote-max-checkpoints</i>
Context	config>system>rollback
Description	Configures the maximum number of rollback checkpoint files when the rollback-location is remote (for example, ftp).
Default	remote-max-checkpoints 10
Parameters	<i>remote-max-checkpoints</i> — 1 to 200

2.13.2.6 Management Infrastructure Control Commands

management

Syntax	management {cli}
Context	config>system
Description	This command enables the context to configure management interface parameters.
Default	N/A
Parameters	cli — allows configuration of parameters related to basic CLI commands for datastore infrastructure operation and behavior

configuration

Syntax	configuration
Context	config>system>management
Description	This command enables the context to configure parameters related to configuration data.
Default	N/A

immediate

Syntax	[no] immediate
Context	config>system>management>configuration
Description	<p>This command enables writeable access in the configure CLI branch.</p> <p>The no form of this command, when configured under the management cli context, blocks writeable access and configuration changes in the configure CLI branch. This causes the running configuration datastore from the configure CLI branch to be read-only.</p> <p>This command can be used to enforce the use of candidate configuration and the commit command, instead of allowing immediate mode line-by-line configuration changes.</p>
Default	immediate (configuration changes are allowed in the configure CLI branch)

2.13.2.7 Show Commands

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

alias

Syntax	alias
Context	<root>
Description	This command displays a list of existing aliases.
Default	N/A
Output	The following table describes alias output fields:

Table 24 Show Alias Output Fields

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

Sample Output

```
A:ALA-103>config>system# show alias
```

```
=====
Alias-Name                Alias-command-name
=====
sri                        show router interface
sse                        show service service-using epipe
ssvpls                     show service service-using vpls
ssvprn                     show service service-using vprn
ssi                        show service service-using ies
-----
Number of aliases : 5
=====
A:ALA-103>config>system#
```


3 File System Management

3.1 In This Chapter

This chapter provides information about file system management.

Topics in this chapter include:

- [The File System](#)
 - [Compact Flash Devices](#)
 - [URLs](#)
 - [Wildcards](#)
- [File Management Tasks](#)
 - [Modifying File Attributes](#)
 - [Creating Directories](#)
 - [Copying Files](#)
 - [Moving Files](#)
 - [Deleting Files and Removing Directories](#)
 - [Displaying Directory and File Information](#)

3.2 The File System

The SR OS 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, display file or directory contents and the image version.

Although some of the storage devices on routers are not actually compact flash devices (for example, cf1: on the 7950 XRS is an internal SSD), we refer to all storage devices as compact flash.

3.2.1 Compact Flash Devices

The file system is based on a DOS file system (with an optional Reliance file system). In the 7750 SR and 7450 ESS, each control processor can have up to three compact flash devices numbered one through three. In the 7950 XRS, each CCM has an SSD and up to two compact flash devices. The names for these devices are:

- cf1:
- cf2:
- cf3:

The above device names are *relative* device names as they refer to the devices local to the control processor with the current console session. As in the DOS file system, the colon (":") at the end of the name indicates it is a device.

The three compact flash devices on the 7450 ESS and 7750 SR OS are removable and have an administrative state (shutdown/no shutdown).

The cf2: and cf3: compact flash devices on the 7950 XRS routers are removable and have an administrative state (shutdown/no shutdown). cf1: is an internal SSD.



Note: To prevent corrupting open files in the file system, you should only remove a compact flash that is administratively shutdown. The SR OS gracefully closes any open files on the device, so it can be safely removed.

3.2.2 URLs

The arguments for the SR OS file commands are modeled after standard universal resource locator (URL). A URL refers to a file (a *file-url*) or a directory (a *directory-url*).

The SR OS 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 are listed in [Table 25](#).

Table 25 URL Types and Syntax

URL Type	Syntax	Notes
<i>local-url</i>	<i>[cflash-id:]path</i>	<i>cflash-id</i> is the compact flash device name. Values: cf1:, cf2:, cf3:

Table 25 URL Types and Syntax (Continued)

URL Type	Syntax	Notes
<i>ftp-url</i>	ftp:// <i>[username[:password]@]host</i> # <i>path</i>	An absolute ftp path from the root of the remote file system. <i>username</i> is the ftp user name <i>password</i> is the ftp user password <i>host</i> is the remote host <i>path</i> is the path to the directory or file
	ftp:// <i>[username[:password]@]host</i> #./ <i>path</i>	A relative ftp path from the user's home directory. Note the period and slash ("./") in this syntax compared to the absolute path.
<i>tftp-url</i>	tftp:// <i>host</i> / <i>path</i> / <i>filename</i>	tftp is only supported for operations on file-urls.

On the 7750 SR and 7950 XRS, if the host portion of the URL is an IPv6 address, then the address should be enclosed in square brackets. For example:

```
ftp://user:passw@[3ffe::97]/./testfile.txt
```

```
tftp://[1111:2222:3333:4444:5555:6666:7777:8888]/./testfile.txt
```

The system accepts either forward slash (/) or backslash (\) characters to delimit directory and/or filenames in URLs. Similarly, the SR OS SCP client application can use either slash or backslash characters, but not all SCP clients treat backslash characters as equivalent to slash characters. In particular, UNIX systems will often times interpret the backslash character as an escape character. This can cause problems when using an external SCP client application to send files to the SCP server. If the external system treats the backslash like an escape character, the backslash delimiter will get stripped by the parser and will not be transmitted to the SCP server.

For example, a destination directory specified as "cf1:\dir1\file1" will be transmitted to the SCP server as "cf1: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.

3.2.3 Wildcards

The platform SROS 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:

```

A:ALA-1>file cf3:\ # copy test*.cfg
siliconvalleycf1:\testfile.cfg
1 file(s) copied.
A:ALA-1>file cf3:\ # cd siliconvalley
A:ALA-1>file cf3:\siliconvalley\ # dir
Volume in drive cf1 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.
A:ALA-1>file cf3:\siliconvalley\ #

```

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

Another example of wildcard usage:

```

A:21# show router mpls lsp 1-63-8*
=====
MPLS LSPs (Originating)
=====
LSP Name                               To                               Fastfail
Adm   Opr                               To                               Fastfail
Config
-----
1-63-8-cc                               213.224.245.8                     No
Up     Dwn                               To                               Fastfail
1-63-8-cw                               213.224.245.8                     No
Up     Dwn
-----
LSPs : 2
=====
A:21#

```

All the commands can operate on the local file system. [Table 26](#) indicates which commands also support remote file operations.

Table 26 File Command Local and Remote File System Support

Command	local-url	ftp-url	tftp-url
attrib	X		
cd	X	X	
copy	X	X	X
delete	X	X	
dir	X	X	

Table 26 File Command Local and Remote File System Support

Command	local-url	ftp-url	tftp-url
md		X	
move	X	X	
rd		X	
repair			
scp	source only		
type	X	X	X
version	X	X	X
shutdown			

3.3 File Management Tasks

The following sections are basic system tasks that can be performed.

Note that when a file system operation is performed with the **copy**, **delete**, **move**, **rd**, or **scp** commands that can potentially delete or overwrite a file system entry, a prompt appears to confirm the action. The **force** keyword performs the copy, delete, move, rd, and scp actions without displaying the confirmation prompt.

- [Modifying File Attributes](#)
- [Creating Directories](#)
- [Copying Files](#)
- [Moving Files](#)
- [Deleting Files and Removing Directories](#)
- [Displaying Directory and File Information](#)
- [Repairing the File System](#)

3.3.1 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 shows an example of the command syntax:

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

The following example shows the file configuration:

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

3.3.2 Creating Directories

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

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

Use the CLI syntax displayed below to modify file attributes:

CLI Syntax: file>
 md file-url

The following is an example of the command syntax:

```
file cf1:\ # md test1file cf1:\ # cd test1
file cf1:\test1\ # md test2
file cf1:\test1\ # cd test2
file cf1:\test1\test2\ # md test3
file cf1:\test1\test2\ # cd test3
file cf1:\test1\test2\test3 #
```

3.3.3 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 router. The destination file has to be of 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:

```
A:ALA-1>file cf1:\ # copy
104.cfgcf1:\test1\test2\test3\test.cfg

A:ALA-1>file cf1:\ # scp file1
admin@192.168.x.x:cf1:\file1

A:ALA-1>file cf1:\ # scp file2 user2@192.168.x.x:/user2/
file2

A:ALA-1>file cf1:\ # scp cf2:/file3
admin@192.168.x.x:cf1:\file3
```

3.3.4 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: A:ALA-1>file cf1:\test1\test2\test3\ # move test.cfg
cf1:\test1
cf1:\test1\test2\test3\test.cfg
A:ALA-1>file cf1:\test1\test2\test3\ # cd ..
A:ALA-1>file cf1:\test1\test2\ # cd ..
A:ALA-1>file cf1:\test1\ # dir

```
Directory of cf1:\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.  
A:ALA-1>file cf1:\test1\ #
```

3.3.5 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 and/or subdirectories, use the **rd /s** 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:

```
A:ALA-1>file cf1:\test1\ # delete test.cfg  
A:ALA-1>file cf1:\test1\ # delete abc.cfg  
A:ALA-1>file cf1:\test1\test2\ # cd test3  
A:ALA-1>file cf1:\test1\test2\test3\ # cd ..  
A:ALA-1>file cf1:\test1\test2\ # rd test3  
A:ALA-1>file cf1:\test1\test2\ # cd ..  
A:ALA-1>file cf1:\test1\ # rd test2  
A:ALA-1>file cf1:\test1\ # cd ..  
A:ALA-1>file cf1:\ # rd test1  
A:ALA-1>file cf1:\ #
```

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

CLI Syntax: file

```
rd file-url rf
```

3.3.6 Displaying Directory and File Information

Use the **dir** command to display a list of files on a file system. The **type** command displays the contents of a file. The **version** command displays the version of a *.tim or iom.tim file. (iom.tim file is used for the XCM on the 7950 XRS).

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 shows an example of the command syntax:

```
A:ALA-1>file cfl:\ # dir
Volume in drive cfl on slot A has no label.
Directory of cfl:\
01/01/1980  12:00a                7597 test.cfg
01/01/1980  12:00a                 957 b.
08/19/2001  02:14p            230110 BOOTROM.SYS
01/01/1980  12:00a                 133 NVRAM.DAT
04/03/2003  05:32a                1709 103.ndx
01/28/2003  05:06a                1341 103.cftg.ndx
01/28/2003  05:06a            20754 103.cftg
04/05/2003  02:20a      <DIR>      test
                15 File(s)                338240 bytes.
                3 Dir(s)                  1097728 bytes free.

A:ALA-1>file cfl:\ # type fred.cfg
# Saved to /cflash1/fred.cfg
# Generated THU FEB 21 01:30:09 2002 UTC
exit all
config
#-----
# Chassis Commands
#-----
card 2 card-type faste-tx-32
exit
#-----
# Interface Commands
#-----
# Physical port configuration
interface faste 2/1
    shutdown
    mode network
exit
interface faste 2/2
    shutdown
exit
interface faste 2/3
```

```
shutdown
exit
interface faste 2/4
A:ALA-1>file cf1:\ # version boot.tim
TiMOS-L-1.0.B3-8
A:ALA-1>file cf1:\ #
```

3.3.7 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 [cflash-id]

The following example shows the command syntax:

```
A:ALA-1>file cf3:\ # repair
Checking drive cf3: on slot A for errors...
Drive cf31: on slot A is OK.
```

3.4 File Command Reference

3.4.1 Command Hierarchy

3.4.1.1 File 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** [*cflash-id*] [**reliable**]
 - **md** *file-url*
 - **move** *old-file-url new-file-url* [**force**]
 - **rd** *file-url rf*
 - **rd** *file-url* [**force**]
 - **repair** [*cflash-id*]
 - **scp** *local-file-url destination-file-url* [**router router-instance**] [**force**]
 - **scp** *local-file-url destination-file-url* [**force**] **service** *service-name*
 - [**no**] **shutdown** [**active**] [**standby**]
 - [**no**] **shutdown** *cflash-id*
 - **type** *file-url*
 - **version** *file-url* [**check**]
 - **vi** *local-url*

3.4.2 Command Descriptions

3.4.2.1 File System Commands

shutdown

Syntax	[no] shutdown [active] [standby] [no] shutdown <i>cflash-id</i>
Context	file
Description	This command shuts down (unmounts) the specified CPM(s).

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

Use the **no shutdown** [cflash-id] command to enable a compact flash (cf1:, cf2:, or cf3:) on the CPM/CFM/CCM. The **no shutdown** command can be issued for a specific slot when no compact flash is present. When a flash card is installed in the slot, the card will be activated upon detection.

In redundant systems, use the **no shutdown** command on cf3: on both SF/CPMs or CCMs in order to facilitate synchronization. See the [synchronize](#) command.



Note: The **shutdown** command must be issued prior to removing a flash card. If no parameters are specified, then the drive referred to by the current working directory will be shut down.

LED Status Indicators

[LED Status Indicators](#) lists the possible states for the compact flash and their LED status indicators.

Table 27 LED Status Indicators

State	Description
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. Note: Do not remove the compact flash during a read/write operation.
Flash defective	If a compact flash is defective, the respective LED blinks amber to reflect the error condition and a trap is raised.
Flash drive shut down	When the compact flash drive is shut down and a compact flash present, the LED is lit amber. In this state, the compact flash can be ejected.
No compact flash present, drive shut down	If no compact flash is present and the drive is shut down the LED is unlit.
No compact flash present, drive enabled	If no compact flash is present and the drive is not shut down the LED is unlit.
Ejecting a compact flash	The compact flash drive should be shut down before ejecting a compact flash card. The LED should turn to solid (not blinking) amber. This is the only mode to safely remove the flash card. If a compact flash drive is not shut down before a compact flash is ejected, the LED blinks amber for approximately 5 seconds before shutting off.

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 administratively enabled
Parameters	<i>cflash-id</i> — specifies the compact flash slot ID to be shut down or enabled. If <i>cflash-id</i> is specified, the drive is shut down or enabled. If no <i>cflash-id</i> is specified, the drive referred to by the current working directory is assumed. If a slot number is not specified, then the active CPM/CFM is assumed. Default the current compact flash device Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B: active — all drives on the active CPM are shutdown or enabled standby — all drives on the standby CPM are shutdown or enabled When both active and standby keywords are specified, then all drives on both CPM are shutdown.

3.4.2.2 File Commands

file

Syntax	file
Context	root
Description	the context to enter and 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. Default N/A

attrib

Syntax	attrib [+r -r] file-url attrib
Context	file

Description	<p>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 (*).</p> <p>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 implies that the -r is set and that the file is read-write-all. For example:</p> <pre>ALA-1>file cf3:\ # attrib cf3:\bootlog.txt cf3:\bof.cfg cf3:\boot.ldr cf3:\sr1.cfg cf3:\test cf3:\bootlog_prev.txt cf3:\BOF.SAV</pre>								
Default	N/A								
Parameters	<p><i>file-url</i> — the URL for the local file</p> <p>Values</p> <table><tr><td><i>local-url remote-url</i></td><td>255 chars max</td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>]/[<i>file-path</i>]</td></tr><tr><td><i>remote-url</i></td><td>[ftp://<i>login:pswd@remote-locn</i>]/[<i>file-path</i>]</td></tr><tr><td colspan="2">cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:</td></tr></table> <p>+r — sets the read-only attribute on the specified file</p> <p>-r — clears/resets the read-only attribute on the specified file</p>	<i>local-url remote-url</i>	255 chars max	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:	
<i>local-url remote-url</i>	255 chars max								
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]								
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]								
cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:									

cd

Syntax	cd [<i>file-url</i>]								
Context	file								
Description	This command displays or changes the current working directory in the local file system.								
Default	N/A								
Parameters	<p><i>file-url</i> — the file URL</p> <table><tr><td><i>local-url remote-url</i></td><td>255 chars max</td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>]/[<i>file-path</i>]</td></tr><tr><td><i>remote-url</i></td><td>[ftp://<i>login:pswd@remote-locn</i>]/[<i>file-path</i>]</td></tr><tr><td colspan="2">cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:</td></tr></table>	<i>local-url remote-url</i>	255 chars max	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:	
<i>local-url remote-url</i>	255 chars max								
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]								
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]								
cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:									

If no *file-url* is entered, the current working directory is displayed.

.. — 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 <i>source-file-url</i> <i>dest-file-url</i> [force]
Context	file
Description	<p>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.</p> <p>When a file is copied to a destination with the same file name, the original file is overwritten by the new file specified in the operation. The following prompt appears if the destination file already exists:</p> <p>“Overwrite destination file (y/n)?”</p> <p>For example:</p> <p>To copy a file named srcfile in a directory called test on cf2 in slot B to a file called destfile in a directory called production on cf1 in slot A, the syntax is:</p> <pre>sr1>file cf2:\ # copy cf2-B/test/srcfile cf1-A/production/destfile</pre> <p>To FTP a file named 121201.cfg in directory mydir stored on cf1 in slot A to a network FTP server with IP address 131.12.31.79 in a directory called backup with a destination file name of 121201.cfg, the FTP syntax is:</p> <pre>copy cf1-A/mydir/121201.cfg 131.12.31.79/backup/121201.cfg</pre>
Default	N/A
Parameters	<p><i>source-file-url</i> — the location of the source file or directory to be copied</p> <p><i>dest-file-url</i> — the destination of the copied file or directory</p> <p>force — forces an immediate copy of the specified file(s). Executes the command without displaying a user prompt message.</p>

delete

Syntax	delete <i>file-url</i> [force]
Context	file

Description	<p>This command deletes the specified file.</p> <p>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:</p> <p>“Delete file <filename> (y/n)?”</p>								
Default	N/A								
Parameters	<p><i>file-url</i> — the file name to delete</p> <p>Values</p> <table> <tr> <td><i>local-url</i> <i>remote-url</i></td><td>255 chars max</td></tr> <tr> <td><i>local-url</i></td><td>[<i>cflash-id</i>]/[<i>file-path</i>]</td></tr> <tr> <td><i>remote-url</i></td><td>[ftp://<i>login:pswd@remote-locn</i>]/[<i>file-path</i>]</td></tr> <tr> <td colspan="2">cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:</td></tr> </table> <p>force — forces an immediate deletion of the specified file(s). The command file delete * force deletes all the wildcard matching files without displaying a user prompt message.</p>	<i>local-url</i> <i>remote-url</i>	255 chars max	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:	
<i>local-url</i> <i>remote-url</i>	255 chars max								
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]								
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]								
cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:									

dir

Syntax	dir [<i>file-url</i>] [sort-order { d n s }] [reverse]						
Context	file						
Description	This command displays a list of files and subdirectories in a directory.						
Default	N/A						
Parameters	<p><i>file-url</i> — the path or directory name</p> <p>Use the <i>file-url</i> with the optional wildcard (*) to reduce the number of files to list.</p> <p>Default lists all files in the current working directory</p> <p>sort-order {d n s} — specifies the sort order</p> <p>Values</p> <table> <tr><td>d</td><td>— date</td></tr> <tr><td>n</td><td>— name</td></tr> <tr><td>s</td><td>— size</td></tr> </table> <p>reverse — reverses the sort order</p>	d	— date	n	— name	s	— size
d	— date						
n	— name						
s	— size						
Output							
Sample Output							


```
A:cses-E12>file cf3:\ # dir
- dir [<file-url>] [sort-order { d | n | s}] [reverse]

<file-url>          : <local-url>|<remote-url>
  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[-interface]
                     x:x:x:x:x:x:d.d.d.d[-interface]
                     x - [0..FFFF]H
                     d - [0..255]D
                     interface - 32 chars max, for link
                     local addresses
  cflash-id         - cf1:|cf1-A:|cf1-B:|cf2:|cf2-A:|
                     cf2-B:|cf3:|cf3-A:|cf3-B:

< d | n | s >       : Sort order: d - date, n - name, s - size
<reverse>          : keyword - reverse order
A:cses-E12>file cf3:\ # dir
```

format

Syntax	format [<i>cflash-id</i>] [<i>reliable</i>]
Context	root>file
Description	This command formats the compact flash. The compact flash must be shut down before starting the format.
Default	N/A
Parameters	<i>cflash-id</i> — the compact flash type <p>Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</p> <p>reliable — enables the reliance file system and disables the default DOS file system. This option is valid only on compact flashes 1 and 2.</p>

md

Syntax	md <i>file-url</i>
Context	file
Description	This command creates a new directory in a file system. <p>Directories can only be created one level at a time.</p>

Default	N/A
Parameters	<i>file-url</i> — the directory name to be created
	Values
	<i>local-url</i> <i>remote-url</i> 255 chars max
	<i>local-url</i> [<i>cflash-id</i>]/[<i>file-path</i>]
	<i>remote-url</i> [ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]
	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

move

Syntax	move <i>old-file-url</i> <i>new-file-url</i> [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)?”

Default	N/A
Parameters	<i>old-file-url</i> — the file or directory to be moved
	Values
	<i>local-url</i> <i>remote-url</i> 255 chars max
	<i>local-url</i> [<i>cflash-id</i>]/[<i>file-path</i>]
	<i>remote-url</i> [ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]
	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

new-file-url — the new destination to place the *old-file-url*

	Values
	<i>local-url</i> <i>remote-url</i> 255 chars max
	<i>local-url</i> [<i>cflash-id</i>]/[<i>file-path</i>]
	<i>remote-url</i> [ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]
	cf1:,cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

force — forces an immediate move of the specified file(s)

The **file move force** command moves the specified file(s) without displaying a user prompt message.

rd

Syntax	rd <i>file-url</i> rf rd <i>file-url</i> [force]														
Context	file														
Description	<p>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.</p> <p>If the directory contains files and/or subdirectories, the rf parameter must be used to remove the directory.</p> <p>Example:</p> <pre>A:nE1>file cf1:\ # rd test Are you sure (y/n)? y Deleting directory cf1:\test ..MINOR: CLI Cannot delete cf1:\test. A:nE1>file cf1:\ # rd test force Deleting directory cf1:\test .MINOR: CLI Cannot delete cf1:\test. A:nE1>file cf1:\ # rd testbase rf Deleting all subdirectories and files in specified directory. y/n ?y Deleting directory cf1:\testbase\testbase1 ..OK Deleting directory cf1:\test ..OK</pre>														
Default	N/A														
Parameters	<p><i>file-url</i> — the directory to be removed</p> <p>Values</p> <table><tr><td><i>local-url</i> <i>remote-url</i></td><td></td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each</td></tr><tr><td><i>remote-url</i></td><td>[ftp://<i>login:pswd@remote-locn</i>/][<i>file-path</i>] 247 chars max directory length 99 chars max each</td></tr><tr><td><i>remote-locn</i></td><td>[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]</td></tr><tr><td><i>ipv4-address</i></td><td>a.b.c.d</td></tr><tr><td><i>ipv6-address</i></td><td>x:x:x:x:x:x:x[-<i>interface</i>] x:x:x:x:x:x.d.d.d.d[-<i>interface</i>] x - [0 to FFFF]H d - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses</td></tr><tr><td><i>cflash-id</i></td><td>cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</td></tr></table>	<i>local-url</i> <i>remote-url</i>		<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each	<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i> /][<i>file-path</i>] 247 chars max directory length 99 chars max each	<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]	<i>ipv4-address</i>	a.b.c.d	<i>ipv6-address</i>	x:x:x:x:x:x:x[- <i>interface</i>] x:x:x:x:x:x.d.d.d.d[- <i>interface</i>] x - [0 to FFFF]H d - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses	<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
<i>local-url</i> <i>remote-url</i>															
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each														
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i> /][<i>file-path</i>] 247 chars max directory length 99 chars max each														
<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]														
<i>ipv4-address</i>	a.b.c.d														
<i>ipv6-address</i>	x:x:x:x:x:x:x[- <i>interface</i>] x:x:x:x:x:x.d.d.d.d[- <i>interface</i>] x - [0 to FFFF]H d - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses														
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:														

rf — forces a recursive delete

force — forces an immediate deletion of the specified directory. The **rd file-url force** command executes the command without displaying a user prompt message.

repair

Syntax	repair [<i>cf</i> <i>flash-id</i>]
Context	file
Description	This command checks a compact flash device for errors and repairs any errors found.
Default	N/A
Parameters	<i>cf</i> <i>flash-id</i> — specifies the compact flash slot ID to be shut down or enabled. When a specific <i>cf</i> <i>flash-id</i> is specified, then that drive is shut down. If no <i>flash-id</i> 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.
	Default the current compact flash device
	Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

scp

Syntax	<code>scp local-file-url destination-file-url [router router-instance] [force]</code> <code>scp local-file-url destination-file-url [force] service service-name</code>
Context	file
Description	This command copies a local file to a remote host file system. It uses <code>ssh</code> for data transfer, and uses the same authentication and provides the same security as <code>ssh</code> . The following prompt appears: “Are you sure (y/n)?” The destination must specify a user and a host.
Default	N/A
Parameters	<i>local-file-url</i> — the local source file or directory Values [<i>cflash-id</i>]/[<i>file-path</i>): up to 256 characters <i>destination-file-url</i> — the destination file Values <i>destination-file-*</i> : <i>user@hostname:file-path</i> - [255 chars max] <i>user</i> 32 chars max <i>hostname</i> [<i>dns-name</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]

<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x::x::x::x::x::x[-interface]</i> <i>x::x::x::x::d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D <i>interface</i> - 32 chars max, mandatory for link local addresses
<i>dns-name</i>	128 chars max
<i>file-path</i>	200 chars max

user — the SSH user
host — the remote host IP address or DNS name
file-path — the destination path
router-instance — specifies the router name or service ID

Values

<i>router-name</i>	Base, management
<i>service-id</i>	1 to 2147483647

Default Base

force — forces an immediate copy of the specified file. The command **file scp** *local-file-url destination-file-url* [**router** *router-instance*] **force** executes the command without displaying a user prompt message.

service *service-name* — specifies the service name up to 64 characters in length

type

Syntax	type <i>file-url</i>
Context	file
Description	This command displays the contents of a text file.
Default	N/A
Parameters	<i>file-url</i> — the file contents to display

Values

<i>local-url</i> <i>remote-url</i>	
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each

<i>remote-url</i>	[{ftp:// tftp://}login:pswd@remote-locn/ [file-path] 255 chars max directory length 99 chars max each
<i>remote-locn</i>	[hostname ipv4-address ipv6-address]
<i>ipv4-address</i>	a.b.c.d
<i>ipv6-address</i>	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, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:

version

Syntax	version <i>file-url</i> [check]
Context	file
Description	This command displays the version of an SR OS *.tim or iom.tim file. The iom.tim file is used for the XCM on the 7950 XRS.
Default	N/A
Parameters	<i>file-url</i> — the file name of the target file

Values

<i>local-url</i> <i>remote-url</i>	255 characters maximum
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]
<i>remote-url</i>	[{ftp:// tftp://}login:pswd@remote-locn/][<i>file-path</i>]
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

check — validates the.tim file

Output

Sample Output

```
A:Redundancy>file cf3:\ # version ftp://test:1234@xxx.xxx.xxx.xx/usr/global/images/
6.1/R4/cpm.tim
TiMOS-C-6.1.R4 for 7750
Thu Oct 30 14:21:09 PDT 2008 by builder in /rel6.1/b1/R4/panos/main
A:Redundancy>file cf3:\ # version check ftp://test:1234@xxx.xxx.xxx.xx/usr/global/
images/6.1/R4/cpm.tim
TiMOS-C-6.1.R4 for 7750
```

```
Thu Oct 30 14:21:09 PDT 2008 by builder in /rel6.1/b1/R4/panos/main
Validation successful
A:Redundancy>file cf3:\ #
```

vi

Syntax	vi <i>local-url</i>
Context	file
Description	Edit files using the vi editor. For more information, refer to VI Editor .
Default	N/A
Parameters	<i>local-url</i> — specifies the local source file or directory
Values	<i>[cflash-id/]file-path</i> <i>cflash-id</i> : cf1:, cf2:, cf3:

4 Boot Options

4.1 In This Chapter

This chapter provides information about configuring boot option parameters.

Topics in this chapter include:

- [System Initialization](#)
 - [Configuration and Image Loading](#)
 - [Persistence](#)
 - [Lawful Intercept](#)
 - [FIPS-140-2 Mode](#)
- [Initial System Startup Process Flow](#)
- [Configuration Notes](#)

4.2 System Initialization

The primary copy of SR OS software is located on a compact flash card. The removable media is shipped with each router and contains a copy of the OS image.



Note:

- The modules contain three slots for removable compact flash cards. The drives are named Compact Flash Slot #1 (cf1), Compact Flash Slot #2 (cf2), and Compact Flash Slot #3 (cf3). Configurations and executable images can be stored on flash cards or an FTP file location. There are six Compact Flash slots on the 7750 SR-c12, three for CFM-A and three for CFM-B.
- The flash card containing the bootstrap and boot option files *must* be installed in Compact Flash Slot #3 (cf3).
- You must have a console connection.

Starting a router begins with hardware initialization (a reset or power cycle). By default, the system searches Compact Flash Slot #3 (cf3) for the boot.ldr file (also known as the bootstrap file). The boot.ldr file is the image that reads and executes the system initialization commands configured in the boot option file (BOF). The default value to initially search for the boot.ldr file on cf3 cannot be modified.

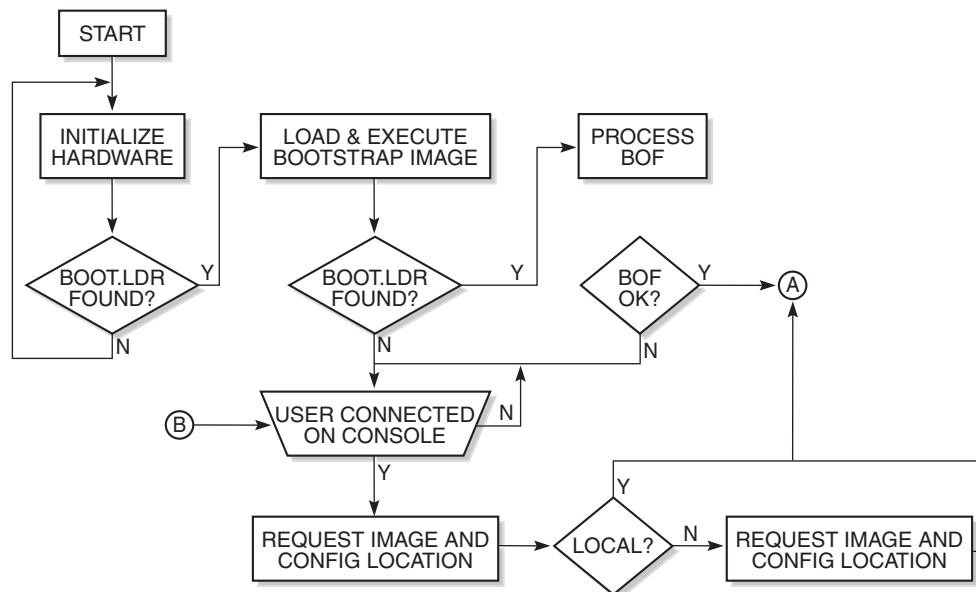
The following is an example of a console display output when the boot.ldr file cannot be located on *cf3*.

```
...
(memory test messages)
(serial number information)
Searching for boot.ldr on local drives:
No disk in cf3
No disk in cf3
No disk in cf3
Error - file boot.ldr not found on any drive
Please insert CF containing boot.ldr. Rebooting in 5 seconds.
```

When the bootstrap image is loaded, the BOF is read to obtain the location of the image and configuration files. The BOF must be located on the same compact flash drive as the boot.ldr file.

Figure 6 displays the system initialization sequence. In the figure, “A” refers to Figure 7, and “B” refers to the list of files on the compact flash.

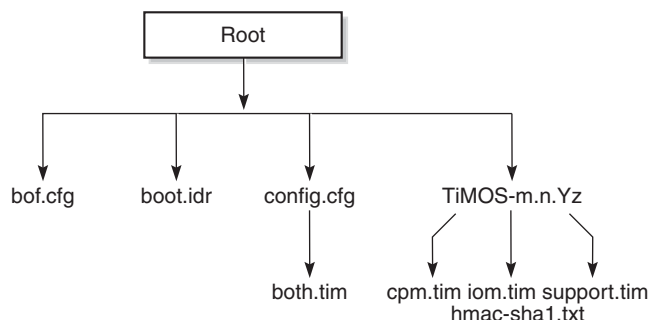
Figure 6 System Initialization - Part 1



25611

Figure 7 displays the compact flash directory structure and file names for the redundant chassis models.

Figure 7 Files on the Compact Flash



25610

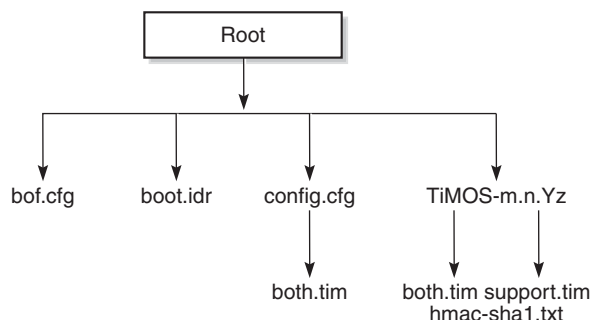
Files on compact flash are:

- bof.cfg — Boot option file
- boot.idr — Bootstrap image
- config.cfg — Default configuration file
- TiMOS-m.n.Yz:
 - m — Major release number
 - n — minor release number
 - Y:A — Alpha release
 - B — Beta release
 - M — Maintenance release
 - R — Released software
 - z — Version number
 - cpm.tim — CPM image file
 - iom.tim — XCM/IOM image file
 - support.tim — required data for SR OS .tim files
 - hmac-sha1.txt (in FIPS-140-2 mode only)



Note: XCM applies to the 7950 XRS only.

Figure 8 displays the compact flash directory structure and file names for the 1-slot and 1-slot non-redundant models (the non-redundant models apply to the 7750 RS only).

Figure 8 Files on the Compact Flash (1-slot and 1-slot non-redundant)

25609

Files on the compact flash (1-slot models) are:

- bof.cfg — Boot option file
- boot.idr — Bootstrap image
- config.cfg — Default configuration file
- TiMOS-m.n.Yz:
 - m — Major release number
 - n — Minor release number
 - Y:A — Alpha release
 - B — Beta release
 - M — Maintenance release
 - R — Released software
 - z — Version number
 - both.tim — CPM and IOM image file
 - support.tim — required data for SR OS .tim files
 - hmac-sha1.txt (in FIPS-140-2 mode only)

The 7750 SR includes a boot option for running the node in a FIPS-140-2 mode. This mode limits the use of cryptographic algorithms on the CPM to only those that are in accordance with the FIPS-140-2 certifications associated with the 7750 SR.

4.2.1 Configuration and Image Loading

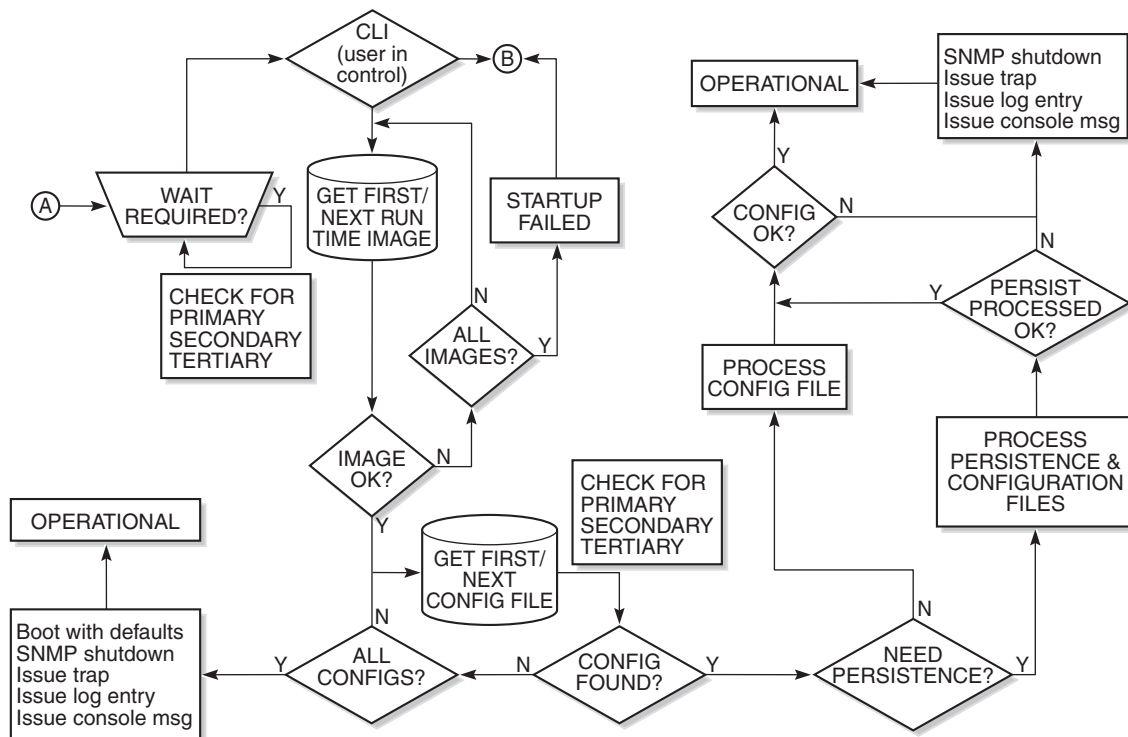
When the system executes the `boot.ldr` file, the initialization parameters from the BOF are processed. Three locations can be configured for the system to search for the files that contains the runtime image. The locations can be local or remote. The first location searched is the primary image location.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

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

The **boot.ldr** can be interrupted during the boot sequence by pressing any key on the CPM console port. The operator must then type **sros** and press **ENTER** within 30 seconds or the **boot.ldr** will continue trying to boot the system. This key sequence ensures that noise or misconfiguration does not inadvertently interrupt the boot sequence. If the operator types **sros** and presses **ENTER** within 30 seconds, they are brought to a console message dialog session prompting the user to enter file locations and other boot information.

When the runtime image is successfully loaded, control is passed from the bootstrap loader to the image. 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, card, MDA, and port configurations, as well as system, routing, and service configurations.

[Figure 9](#) displays the boot sequence.

Figure 9 System Initialization - Part 2

25612

The following displays an example of BOF output:

```

A:ALA-1>bof# show bof
=====
Memory BOF
=====
no autonegotiate
duplex      full
speed       100
address      10.10.xx.xx/20 active
wait         3
primary-image cf3:\both.tim
primary-config cf3:\test123.cfg
primary-dns 192.168.xx.xx
persist      on
dns-domain test.nokia.com
=====
A:ALA-1>bof#

```

4.2.1.1 Persistence

Optionally, 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, path IDs, etc. If persistence is not required and the configuration file is successfully processed, then the system becomes operational. If persist is required, then 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. Note that 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.

4.2.1.2 Lawful Intercept

Lawful Intercept (LI) describes a process to intercept telecommunications by which law enforcement authorities can unobtrusively monitor voice and data communications to combat crime and terrorism with higher security standards of lawful intercept capabilities in accordance with local law and after following due process and receiving proper authorization from competent authorities. The interception capabilities are sought by various telecommunications providers.

As lawful interception is subject to national regulation, requirements vary from one country to another. This implementation satisfies most national standard's requirements. LI is configurable for all service types.

4.2.1.3 FIPS-140-2 Mode

The 7750 SR includes a configurable parameter in the bof.cfg file to make the node run in FIPS-140-2 mode. When the node boots in FIPS-140-2 mode, the following behaviors are enabled on the node:

- The node performs an HMAC-SHA1 integrity test on the software images .tim files.
- The node limits the use of encryption and authentication algorithms to only those allowed for the associated FIPS-140-2 certification of the 7750-SR.

- Cryptographic module startup tests are executed on the CPM when the node boots to ensure the associated approved FIPS-140-2 algorithms are operating correctly.
- Cryptographic module conditional tests are executed when required during normal operation of associated when using FIPS-140-2 approved algorithms.
- When configuring user-defined encryption or authentication keys, CLI will prompt for the key to be re-entered. If the re-entered key does not match the original, the CLI command will be canceled. This affects several protocols and applications.

To support FIPS-140-2, an HMAC-SHA-1 integrity check is performed to verify the integrity of the software images. The following file is included in the TIMOS-m.n.Yz software bundle containing the hmac-sha-1 signature:

- hmac-sha1.txt

During the loading of the cpm.tim or both.tim, a HMAC-SHA-1 check is performed to ensure that the calculated HMAC-SHA-1 of the loaded image matches that stored in the hmac-sha1.txt file.

The HMAC-SHA-1 check is performed on the data loaded from the .tim file. Note that when configuring the primary-image, secondary-image and tertiary-image, the hmac-sha1.txt file must exist in the same directory as the .tim files. If the load has been verified correctly from the HMAC-SHA-1 integrity check, the load continues to bootup as normal. If the load is not verified by the HMAC-SHA-1 integrity check, the image load will fail.

After the HMAC-SHA-1 integrity check passes, the nodes continues its normal bootup sequence including reading the config.cfg file and loading the configuration. The config.cfg file used to boot the node in FIPS-140-2 mode must not contain any configuration that is not supported in FIPS-140-2 mode. If such configuration is present in the config.cfg file when the node boots, the node will load the config.cfg file until the location of the offending configuration and then halt the configuration at that point. Upon a failure to load the config.cfg file, a failure message is printed on the console.

Enabling FIPS-140-2 restricts the ability to configure and use cryptographic algorithms and functions that are not FIPS approved. FIPS-140-2 impacts the ability to configure SSH, SNMP and certificates. Please refer to the 7450 ESS, 7750 SR, and 7950 XRS System Management Guide for details of FIPS-140-2 related items.

In addition, signature algorithms of the following combinations only are approved for FIPS:

- FIPS-140 Approved - Digital Signature Standard (DSS)
 - DSA

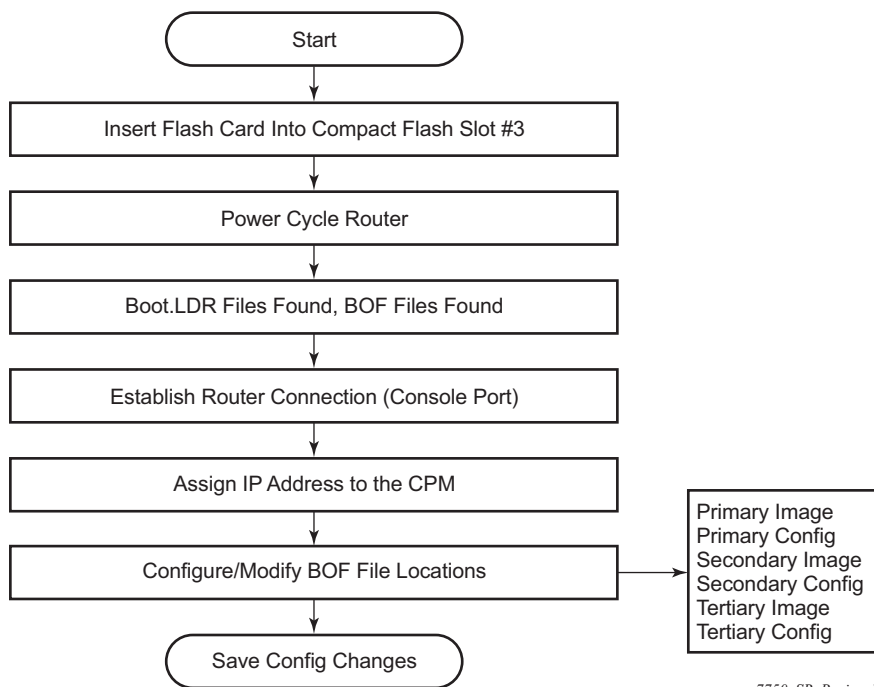
- RSA
- ECDSA
- FIPS-140 Approved - Secured Hash Standard (SHS)
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512

Any other combination is not supported in FIPS mode. Using other FIPS signature algorithms in certificates affecting IPSec can cause tunnels to fail. Restrictions to cryptographic algorithms are listed in the *System Configuration guide*.

4.3 Initial System Startup Process Flow

Figure 10 displays the process start your system. Note that this example assumes that the boot loader and BOF image and configuration files are successfully located.

Figure 10 System Startup Flow



7750_SR_Basics_10

4.4 Configuration Notes

This section describes BOF configuration caveats.

- For router initialization, the compact flash card must be installed in the Compact Flash #3 slot.
- The loading sequence is based on the order in which it is placed in the configuration file. It is loaded as it is read in at boot time.

4.5 Configuring Boot Options File with CLI

This section provides information to configure BOF parameters with CLI.

Topics in this section include:

- [BOF Configuration Overview](#)
- [Basic BOF Configuration](#)
- [Common Configuration Tasks](#)
- [Configuring BOF Parameters](#)
- [Service Management Tasks](#)
 - [Viewing the Current Configuration](#)
 - [Modifying and Saving a Configuration](#)
 - [Saving a Configuration to a Different Filename](#)
 - [Rebooting](#)

4.6 BOF Configuration Overview

Nokia 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:

- Step 1.** Sets up the CPM/CCM Ethernet port (speed, duplex, auto).
- Step 2.** Assigns the IP address for the CPM/CCM Ethernet port.
- Step 3.** Creates static routes for the CPM/CCM Ethernet port.
- Step 4.** Sets the console port speed.
- Step 5.** Configures the Domain Name System (DNS) name and DNS servers.
- Step 6.** Configures the primary, secondary, tertiary configuration source.
- Step 7.** Configures the primary, secondary, and tertiary image source.
- Step 8.** Configures operational parameters.

4.7 Basic BOF Configuration

The parameters which specify location of the image filename that the router will try 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 is a sample of a basic BOF configuration.

```
A:SR-45# show bof
=====
BOF (Memory)
=====
primary-image cf3:/4.0.R20
primary-config cf3:/ospf_default.cfg
address 138.120.189.53/24 active
static-route 138.120.0.0/16 next-hop 138.120.189.1
static-route 172.0.0.0/8 next-hop 138.120.189.1
autonegotiate
duplexfull
speed100
wait3
persiston
console-speed 115200
=====
A:SR-45#
```

4.8 Common Configuration Tasks

The following sections are basic system tasks that must be performed.

- [Searching for the BOF](#)
 - [Accessing the CLI](#)
 - [Console Connection](#)
- [Configuring BOF Parameters](#)

For details about hardware installation and initial router connections, refer to the specific router hardware installation guide.

4.8.1 Searching for the BOF

The BOF should be on the same drive as the boot loader file. If the system cannot load or cannot find the BOF then the system checks whether the boot sequence was manually interrupted. The system prompts for a different image and configuration location.

The following example shows an example of the output when the boot sequence is interrupted.

...

Hit a key within 3 seconds to change boot params...

You must supply some required Boot Options. At any prompt, you can type:

"restart" - restart the query mode.
"reboot" - reboot.
"exit" - boot with 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:/timos1.0R1
ftp://user:passwd@192.168.xx.xxx/./timos1.0R1
tftp://192.168.xx.xxx/./timos1.0R1

The existing Image URL is 'ftp://vxworks:vxw0rks@192.168.xx.xxx/./rel/0.0/xx'

Press ENTER to keep it.

Software Image URL:

Using: 'ftp://vxworks:vxw0rks@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

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://vxworks:vxw0rks@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

4.8.2 Accessing the CLI

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

- When the CPM/CFM/CCM is installed, and power to the chassis is turned on, the SR OS software automatically begins the boot sequence.
- When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

4.8.2.1 Console Connection

To establish a console connection, you will need the following:

- An ASCII terminal or a PC running terminal emulation software set to the parameters shown in the table below.
- A standard serial cable with a male DB9.

Table 28 Console Configuration Parameter Values

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

To establish a console connection:

- Step 1.** Connect the terminal to the Console port on the CPM/CFM/CCM using the serial cable.
- Step 2.** Power on the terminal.
- Step 3.** Establish the connection by pressing the <Enter> key a few times on your terminal keyboard.
- Step 4.** At the router prompt, enter the login and password.
The default login is admin.
The default password is admin.

4.9 Configuring BOF Parameters

The following example shows a BOF configuration on a 7750 SR:

```
A:ALA-1>bof# show bof
=====
Memory BOF
=====
no autonegotiate
duplex      full
speed      100
address    10.10.xx.xx/20 active
wait       3
primary-image cf3:\both.tim
primary-config cf3:\test123.cfg
primary-dns 192.168.xx.xx
persist     on
dns-domain  test.nokia.com
=====
A:ALA-1>bof#
```

4.10 Service Management Tasks

This section discusses the following service management tasks:

- [System Administration Commands](#)
 - [Viewing the Current Configuration](#)
 - [Modifying and Saving a Configuration](#)
 - [Deleting BOF Parameters](#)
 - [Saving a Configuration to a Different Filename](#)

4.10.1 System Administration Commands

Use the following administrative commands to perform management tasks.

CLI Syntax: A:ALA-1# admin
 display-config
 reboot [active | standby | upgrade] [hold] [now]
 save [file-url] [detail] [index]

4.10.1.1 Viewing the Current Configuration

Use one of the following CLI commands to display the current configuration. The **detail** option displays all default values. The **index** option displays only the persistent indices. The **info** command displays context-level information.

CLI Syntax: `admin# display-config [detail | index]
info detail`

The following example shows a configuration file for the 7750 SR:

```
A:7750-3>admin# display-config
# TiMOS B-1.0.Ixxx - Copyright (c) 2000-2016 Nokia
# Built on Tues Jan 21 21:39:07 2007 by builder in /rel1.0/xx/panos/main

# Generated WED Jan 31 06:15:29 2007 UTC

exit all
configure
#-----
echo "System Configuration"
#-----
system
    name "7750-3"
    contact "Fred Information Technology"
    location "Bldg.1-floor 2-Room 201"
    cli-code "abcdefg1234"
    coordinates "N 45 58 23, W 34 56 12"
    ccm 1
    exit
    snmp
    exit
    login-control
        idle-timeout 1440
        motd text "7750-3"
    exit
    time
        sntp
            shutdown
        exit
        zone UTC
    exit
    thresholds
        rmon
        exit
    exit
exit...
...
-----
echo "Redundancy Configuration"
#-----
    redundancy
        synchronize boot-env
    exit
...exit all
```

```
# Finished FRI Nov 21 15:06:16 2008 UTC
A:7750#
```

4.10.1.2 Modifying and 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 file names 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.
- Changing the active and standby addresses without reboot standby CPM may cause a boot-env sync to fail.

The following command saves a configuration:

CLI Syntax: `bof# save [cflash-id]`

Example: `A:ALA-1# bof`
 `A:ALA-1>bof# save cf3:`
 `A:ALA-1>bof#`

The following command saves the system configuration:

CLI Syntax: `admin# save [file-url] [detail] [index]`

Example: `A:ALA-1# admin save cf3:\test123.cfg`
 `Saving config.# Saved to cf3:\test123.cfg`
 `... complete`
 `A:ALA-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.

4.10.1.3 Deleting BOF Parameters

You can delete specific 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.

Deleting a BOF address entry is not allowed from a Telnet session.

Use the following CLI syntax to save and remove BOF configuration parameters:

CLI Syntax: `bof# save [cflash-id]`

Example: `A:ALA-1# bof`
 `A:ALA-1>bof# save cf3:`
 `A:ALA-1>bof#`

CLI Syntax: `bof#`
 `no address ip-address/mask [active | standby]`
 `no autonegotiate`
 `no console-speed`
 `no dns-domain`
 `no li-local-save`
 `no li-separate`
 `no primary-config`
 `no primary-dns`
 `no primary-image`
 `no secondary-config`
 `no secondary-dns`
 `no secondary-image`
 `no static-route ip-address/mask next-hop ip-address`
 `no tertiary-config`
 `no tertiary-dns`
 `no tertiary-image`

4.10.1.4 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 the following CLI syntax to save a configuration to a different location:

CLI Syntax: `admin# save [file-url] [detail] [index]`

Example: A:ALA-1>admin# save cf3:\testABC.cfg
 Saving config.# Saved to cf3:\testABC.cfg
 ... complete
 A:ALA-1#

4.10.1.5 Rebooting

When an **admin>reboot** command is issued, routers with redundant CPM are rebooted as well as the XMA's, XCM's, and IOM's. 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 | upgrade] [hold] [now]

Example: A:ALA-1>admin# reboot
 A:DutA>admin# reboot
 Are you sure you want to reboot (y/n)? y
 Resetting...OK
 Alcatel 7xxx Boot ROM. Copyright 2000-2007 Alcatel-
 Lucent.
 All rights reserved. All use is subject to applicable
 license agreements.....

4.11 BOF Configuration Command Reference

4.11.1 Command Hierarchies

4.11.1.1 Configuration Commands

bof

- [no] **address** *ip-prefix/ip-prefix-length* [active | standby]
- [no] **autonegotiate**
- **console-speed** *baud-rate*
- no **console-speed**
- **dns-domain** *dns-name*
- no **dns-domain**
- **duplex** {full | half}
- [no] **fips-140-2**
- [no] **li-local-save**
- [no] **li-separate**
- **persist** {on | off}
- **primary-config** *file-url*
- no **primary-config**
- [no] **primary-dns** *ip-address*
- **primary-image** *file-url*
- no **primary-image**
- **save** [*cflash-id*]
- **secondary-config** *file-url*
- no **secondary-config**
- [no] **secondary-dns** *ip-address*
- **secondary-image** *file-url*
- no **secondary-image**
- **speed** *speed*
- [no] **static-route** *ip-prefix/ip-prefix-length* **next-hop** *ip-address*
- **tertiary-config** *file-url*
- no **tertiary-config**
- [no] **tertiary-dns** *ip-address*
- **tertiary-image** *file-url*
- no **tertiary-image**
- **wait** *seconds*

4.11.2 Command Descriptions

4.11.2.1 File Management Commands

bof

Syntax	bof
Context	<root>
Description	<p>This command creates or edits the boot option file (BOF) for the specified local storage device.</p> <p>A BOF file specifies where the system searches for runtime images, configuration files, and other operational parameters during system initialization.</p> <p>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 <i>bof.cfg</i>.</p> <p>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 management port is changed, the change takes place immediately.</p> <p>Only one entry of the BOF configuration command statement can be saved once the statement has been found to be syntactically correct.</p> <p>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 will not affect the operation of the node.</p> <p>No default boot option file exists. The router boots with the factory default boot sequence and options.</p>
Default	N/A

save

Syntax	save [<i>cflash-id</i>]
Context	bof
Description	<p>This command uses the boot option parameters currently in memory and writes them from the boot option file to the specified compact flash.</p> <p>The BOF must be located in the root directory of the internal or external compact flash drives local to the system and have the mandatory filename of <i>bof.cfg</i>.</p>

If a location is not specified, the BOF is saved to the default compact flash drive (cf3:) on the active CPM (typically the CPM in slot A, but the CPM in slot B could also be acting as the active CPM). The slot name is not case-sensitive. You can use upper or lowercase “A” or “B”.

Command usage:

- **bof save** — saves the BOF to the default drive (cf3:) on the active CPM (either in slot A or B)
- **bof save cf3:** — saves the BOF to cf3: on the active CPM (either in slot A or B)

To save the BOF to a compact flash drive on the standby CPM (for example, the redundant (standby) CPM is installed in slot B), specify -A or -B option.

Command usage:

- **bof save cf3-A:** — saves the BOF to cf3: on CPM in slot A whether it is active or standby
- **bof save cf3-B:** — saves the BOF to cf3: on CPM in slot B whether it is active or standby

The slot name is not case-sensitive. You can use upper 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 CPM. Use the **show card** command to determine the active and standby CPM (A or B).

Default Saves must be explicitly executed. The BOF is saved to cf3: if a location is not specified.

Parameters *flash-id* — the compact flash ID where the *bof.cfg* is to be saved

Values	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
Default	cf3:

4.11.2.2 BOF Processing Control

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 boot option file (BOF).

Only one **wait** command can be defined in the BOF.

Default	wait 3
Parameters	<i>seconds</i> — the time to pause at the start of the boot process, in seconds
Values	1 to10

4.11.2.3 Console Port Configuration

console-speed

Syntax	console-speed <i>baud-rate</i> no console-speed
Context	bof
Description	<p>This command configures the console port baud rate.</p> <p>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.</p> <p>The no form of the command reverts to the default value.</p>
Default	115200 — console configured for 115,200 bps operation
Parameters	<i>baud-rate</i> — the console port baud rate, expressed as a decimal integer
Values	9600, 19200, 38400, 57600, 115200

4.11.2.4 Image and Configuration Management

persist

Syntax	persist { on off }
Context	bof
Description	<p>This command specifies whether the system will 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, path IDs, etc. This reduces resynchronizations of the Network Management System (NMS) with the affected network element.</p>

In the event that **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 will not be saved correctly.



Note:

- Persistency files (.ndx) are 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 will check to ensure that the disk has enough free space. If this there is not enough free space, the persistency will not become active and a trap will be generated. Then, it is up to the operator to free adequate disk space. In the meantime, the system will perform a space availability check every 30 seconds. As soon as the space is available the persistency will become active on the next (30 second) check.

Default persist off

Parameters **on** — create 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 the **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, expressed as a file URL

Values

<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

primary-image

Syntax	primary-image <i>file-url</i> no primary image								
Context	bof								
Description	<p>This command specifies the primary directory location for runtime image file loading.</p> <p>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.</p> <p>All runtime image files (*.tim files) must be located in the same directory.</p> <p>The no form of the command removes the primary-image configuration.</p>								
Default	N/A								
Parameters	<i>file-url</i> — the <i>file-url</i> can be either local (this CPM) or a remote FTP server								
	Values <table> <tr> <td><i>file-url</i></td><td>[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)</td></tr> <tr> <td><i>local-url</i></td><td>[<i>cflash-id</i>][<i>file-path</i>]</td></tr> <tr> <td><i>remote-url</i></td><td>[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]</td></tr> <tr> <td><i>cflash-id</i></td><td>cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</td></tr> </table>	<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)	<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]	<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]	<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)								
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]								
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]								
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:								

secondary-config

Syntax	secondary-config <i>file-url</i> no secondary-config
Context	bof
Description	<p>This command specifies the name and location of the secondary configuration file.</p> <p>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.</p>

Note that 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, expressed as a file URL

Values

<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

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.

All runtime image files (*.tim files) must be located in the same directory.

The **no** form of the command removes the **secondary-image** configuration.

Default N/A

Parameters *file-url* — can be either local (this CPM) or a remote FTP server

Values

<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

tertiary-config

Syntax **tertiary-config** *file-url*
no tertiary-config

Context	bof								
Description	<p>This command specifies the name and location of the tertiary configuration file.</p> <p>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.</p> <p>Note that if an error in the configuration file is encountered, the boot process aborts.</p> <p>The no form of the command removes the tertiary-config configuration.</p>								
Default	N/A								
Parameters	<p><i>file-url</i> — the tertiary configuration file location, expressed as a file URL</p> <p>Values</p> <table><tr><td><i>file-url</i></td><td>[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)</td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>][<i>file-path</i>]</td></tr><tr><td><i>remote-url</i></td><td>[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]</td></tr><tr><td><i>cflash-id</i></td><td>cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</td></tr></table>	<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)	<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]	<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]	<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)								
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]								
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]								
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:								

tertiary-image

Syntax	tertiary-image <i>file-url</i> no tertiary-image						
Context	bof						
Description	<p>This command specifies the tertiary directory location for runtime image file loading.</p> <p>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.</p> <p>All runtime image files (*.tim files) must be located in the same directory.</p> <p>The no form of the command removes the tertiary-image configuration.</p>						
Default	N/A						
Parameters	<p><i>file-url</i> — can be either local (this CPM) or a remote FTP server</p> <p>Values</p> <table><tr><td><i>file-url</i></td><td>[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)</td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>][<i>file-path</i>]</td></tr><tr><td><i>remote-url</i></td><td>[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]</td></tr></table>	<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)	<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]	<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]
<i>file-url</i>	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)						
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>]						
<i>remote-url</i>	[{ftp:// tftp://} <i>login:pswd@remote-locn</i>][<i>file-path</i>]						

cflash-id cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

4.11.2.5 Management Ethernet Configuration

address

Syntax	[no] address <i>ip-prefix/ip-prefix-length</i> [active standby]
Context	bof
Description	<p>This command assigns an IP address to the management Ethernet port on the active CPM in the running configuration and the Boot Option File (BOF) or the standby CPM for systems using redundant CPMs. Deleting a BOF address entry is not allowed from a remote session.</p> <p>Note that changing the active and standby addresses without reboot standby CPM may cause a boot-env sync to fail.</p> <p>The no form of the command deletes the IP address from the CPM Ethernet port.</p>
Default	no address — There are no IP addresses assigned to Ethernet ports.
Parameters	<i>ip-prefix/ip-prefix-length</i> — the destination address of the aggregate route in dotted decimal notation
	Values
<i>ipv4-prefix</i>	<i>a.b.c.d</i> (host bits must be 0)
<i>ipv4-prefix-length</i>	0 to 32
<i>ipv6-prefix</i>	<i>x:x:x:x:x:x:x</i> (eight 16-bit pieces)
	<i>x:x:x:x:x:d.d.d.d</i>
	<i>x:</i> [0 to FFFF]H
	<i>d:</i> [0 to 255]D
<i>ipv6-prefix-length</i>	0 to 128



Note: Ipv6 is applicable to the 7750 SR and 7950 XRS only.

active | standby — specifies which CPM Ethernet address is being configured: the active CPM Ethernet or the standby CPM Ethernet

Default active

autonegotiate

Syntax	[no] autonegotiate
Context	bof
Description	<p>This command enables speed and duplex autonegotiation on the management Ethernet port in the running configuration and the Boot Option File (BOF).</p> <p>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.</p> <p>The no form of the command disables the autonegotiate feature on this port.</p>
Default	N/A
Parameters	limited — specifies ethernet ports to be configurable to use link autonegotiation but with only a single speed/duplex combination advertised. This allows a specific speed/duplex to be guaranteed without having to turn off autonegotiation, which is not allowed for 1000BASE-T.

duplex

Syntax	duplex {full half}
Context	bof
Description	<p>This command configures the duplex mode of the CPM management Ethernet port when autonegotiation is disabled in the running configuration and the Boot Option File (BOF). If the port is configured to autonegotiate this parameter will be ignored.</p>
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	<p>This command is used to configure the node in FIPS-140-2 mode. Before using this command, the operator must ensure that no current configuration exists in the config file that is not supported in FIPS-140-2 mode. Failing to remove unsupported configuration will result in the node being unable to boot up. The node must be rebooted after executing this command in order for the node to begin operating in FIPS-140-2 mode.</p>

Default no fips-140-2

li-local-save

Syntax [no] li-local-save

Context bof

Description This command enables the lawful intercept (LI) configuration to be saved locally.

Default N/A

li-separate

Syntax [no] li-separate

Context bof

Description This command enables separate access to lawful intercept (LI) information.

Default N/A

speed

Syntax speed *speed*

Context bof

Description This command configures the speed for the CPM management Ethernet port when autonegotiation is disabled in the running configuration and the Boot Option File (BOF).

If the port is configured to autonegotiate this parameter is ignored.

Default speed 100 — 100 M/bps operation

Parameters 10 — sets the link to 10 M/bps speed
100 — sets the link to 100 M/bps speed

static-route

Syntax [no] static-route *ip-prefix/ip-prefix-length next-hop ip-address*

Context bof

Description This command creates a **static route** entry for the CPM management Ethernet port in the running configuration and the Boot Option File (BOF).

This command allows manual configuration of static routing table entries. These static routes are only used by traffic generated by the CPM Ethernet port. To reduce configuration, manual address aggregation should be applied where possible.

A static default (0.0.0.0/0 or ::/0) route cannot be configured on the CPM Ethernet port. A maximum of 10 static routes can be configured on the CPM port.

The **no** form of the command deletes the static route.

Default No default routes are configured.

Parameters *ip-prefix/ip-prefix-length* — the destination address of the static route in dotted decimal notation

Values

<i>ip-prefix/ip-prefix-length</i>	ipv4-prefix	a.b.c.d (host bits must be 0)
	ipv4-prefix-le	0 to32
	ipv6-prefix	x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x.d.d.d
		x: [0 to FFFF]H
		d: [0to 255]D
	ipv6-prefix-le	0 to128
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x.d.d.d

<i>ip-address</i>		x: [0 to FFFF]H
		d: [0 to 255]D



Note: Ipv6 is applicable to the 7750 SR and 7950 XRS only.

mask — the subnet mask, expressed as an integer or in dotted decimal notation

Values 1 to32 (mask length), 128.0.0.0 to255.255.255.255 (dotted decimal)

next-hop *ip-address* — the next hop IP address used to reach the destination

4.11.2.6 DNS Configuration Commands

dns-domain

Syntax	dns-domain <i>dns-name</i> no dns-domain
Context	bof
Description	<p>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.</p> <p>The no form of the command removes the domain name from the configuration.</p>
Default	no dns-domain — No DNS domain name is configured.
Parameters	<i>dns-name</i> — specifies the DNS domain name up to 32 characters in length

primary-dns

Syntax	primary-dns <i>ip-address</i> no primary-dns
Context	bof
Description	<p>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.</p> <p>The no form of the command removes the primary DNS server from the configuration.</p>
Default	no primary-dns — no primary DNS server is configured
Parameters	<i>ip-address</i> — the IP or IPv6 address of the primary DNS server

Values

ipv4-address	<i>a.b.c.d</i>
ipv6-address	<i>x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:d.d.d.d[-interface]</i> <i>x: [0 to FFFF]H</i> <i>d: [0 to 255]D</i>
interface	32 chars max, for link local addresses



Note: Ipv6 is applicable to the 7750 SR and 7950 XRS only.

secondary-dns

Syntax	[no] secondary-dns ip-address		
Context	bof		
Description	<p>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.</p> <p>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.</p> <p>The no form of the command removes the secondary DNS server from the configuration.</p>		
Default	no secondary-dns — no secondary DNS server is configured		
Parameters	ip-address — the IP or IPv6 address of the secondary DNS server		
	Values		
	ipv4-address	a.b.c.d	
	ipv6-address	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, for link local addresses	



Note: Ipv6 is applicable to the 7750 SR and 7950 XRS only.

tertiary-dns

Syntax	[no] tertiary-dns ip-address		
Context	bof		
Description	<p>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.</p> <p>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.</p> <p>The no form of the command removes the tertiary DNS server from the configuration.</p>		
Default	no tertiary-dns — no tertiary DNS server is configured		

Parameters	<i>ip-address</i> — the IP or IPv6 address of the tertiary DNS server	
	Values	
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0 to FFFF]H d: [0 to 255]D
	interface	32 chars max, for link local addresses



Note: Ipv6 is applicable to the 7750 SR and 7950 XRS only.

4.12 BOF Show Command Reference

4.12.1 Command Hierarchies

show
— **bof** [*cflash-id* | *booted*]
— **boot-messages**

4.12.2 Command Descriptions

4.12.2.1 BOF Show Commands

The command outputs in the following sections 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 Boot Option File (BOF) executed on 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 upper or lowercase “A” or “B” for the slot name.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

booted — displays the boot option file used to boot the system

Output **Show BOF Fields**

[Table 29](#) describes BOF output fields.

Table 29 Show BOF Output Fields

Label	Description
primary-image	The primary location of the directory that contains the runtime images of both CPM and XCM/IOM.
primary-config	The primary location of the file that contains the configuration.
primary-dns	The primary DNS server for resolution of host names to IP addresses.
secondary-image	The secondary location of the directory that contains the runtime images of both CPM and XCM/IOM.
secondary-config	The secondary location of the file that contains the configuration.

Table 29 Show BOF Output Fields (Continued)

Label	Description
secondary-dns	The secondary DNS server for resolution of host names to IP addresses.
tertiary-image	The tertiary location of the directory that contains the runtime images of both CPM and XCM/IOM.
tertiary-config	The tertiary location of the file that contains the configuration.
address	The IP address and mask associated with the CPM Ethernet port or the secondary CPM port.
tertiary-dns	The tertiary DNS server for resolution of host names to IP addresses.
persist	on — Persistent indexes between system reboots is enabled. off — Persistent indexes between system reboots is disabled.
wait	The time configured for the boot to pause while waiting for console input.
autonegotiate	no autonegotiate — Autonegotiate 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 CPM Ethernet interface.
console speed	The console port baud rate.
dns domain	The domain name used when performing DNS address resolution.
uplinkA-address	Displays the Uplink-A IP address.
uplinkA-port	Displays the primary port to be used for auto-boot.
uplinkA-route	Displays the static route associated with Uplink-A.
uplinkA-vlan	Displays the VLAN ID to be used on Uplink-A.
uplinkB-address	Displays the Uplink-B IP address.
uplinkB-port	Displays the secondary port to be used for auto-boot.
uplinkB-route	Displays the static route associated with Uplink-B.
uplinkB-vlan	Displays the VLAN ID to be used on Uplink-B.
uplink-mode	Displays the uplink mode of the device.
no-service-ports	Displays the ports on which service traffic is not processed.

Table 29 Show BOF Output Fields (Continued)

Label	Description
use-expansion-card-type	Displays the expansion card type.

Sample Output

```

A:ALA-1# show bof cf3:
=====
BOF on cf3:
=====
autonegotiate
primary-image      ftp://test:test@192.168.xx.xx/./both.tim
primary-config     ftp://test:test@192.168.xx.xx/./1xx.cfg
secondary-image    cf1:/i650/
secondary-config   cf1:/config.cfg
address            192.168.xx.xxx/20 active
address            192.168.xx.xxx/20 standby
primary-dns        192.168.xx.xxx
dns-domain         test.test.com
autonegotiate
duplex             full
speed              100
wait               2
persist            off
        console-speed  115200
=====
A:ALA-1#
A:ALA-1# show bof booted
=====
System booted with BOF
=====
primary-image      ftp://test:test@192.168.xx.xx/./both.tim
primary-config     ftp://test:test@192.168.xx.xx/./103.cfg
secondary-image    cf1:/i650/
secondary-config   cf1:/config.cfg
address            192.168.xx.xxx/20 active
address            192.168.xx.xxx/20 standby
primary-dns        192.168.xx.xxx
dns-domain         test.test.com
autonegotiate
duplex             full
speed              100
wait               2
persist            off
        console-speed  115200
=====
A:ALA-1#

```

boot-messages**Syntax boot-messages**

Context	show
Description	This command displays boot messages generated during the last system boot.
Output	

Sample Output for the 7750 SR

```

ALA-## show boot-messages
Boot log started on CPU#0
  Build: X-1.2.B1-7 on Thurs Jan 13 14:49:23 201 by builder
  CPUCTL FPGA version: 2A
Forcing BDB controller to HwSlot 0
Performing Power on Diagnostics
>>>Testing mainboard FPGA chain...
JTAG chain length = 2
All requested FPGAs on chain programmed
>>>Validating SDRAM from 0x21f00000 to 0x22000000
>>>Testing SDRAM from 0x02200000 to 0x21f00000
>>>Testing Compact Flash 1... Slot Empty
>>>Testing Compact Flash 2... Slot Empty
>>>Testing Compact Flash 3... OK (TOSHIBA THNCF128MBA)
Wales peripheral FPGA version is 0x13
Hardware Slot 31
Card type in EEPROM is 0x6, 'england_r1'
MDA #1: HwType 0x02, 'denmark_r1', Serial Number 'de3-52'
MDA #2: HwType 0x16, 'hungary_ds3_e3_12_r1', Serial Number 'hun01-02'
Board Serial Number is 'eng02-15'
Chassis type 4 (sr1) found in BP 1 EEPROM
Chassis Serial Number is '0203210096'
JTAG chain length = 2
All requested FPGAs on chain programmed
Searching for boot.ldr on local drives:
Searching cf3 for boot.ldr...
*****
  Loaded 0x001bc191 bytes from cf3 to 0x80400000
  Decompressing to address 0x0a000000
Starting code...

Total Memory: 512MB Chassis Type: sr1 Card Type: england_r1
TiMOS-L-14.0.B1-217 boot/i386 Nokia 7750 SR Copyright (c) 2000-2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /rel14.0/b1/B1-217/panos/main

TiMOS BOOT LOADER
Time from clock is Thurs Jan 13 08:39:03 2011 UTC
Error: could not open boot messages file.
Boot messages will not be stored.

Looking for cf3:/bof.cfg ... OK, reading

Contents of Boot Options File on cf3:
  primary-image  ftp://vxworks:vxw0rks@192.168.15.1/./rel/0.0/I129
  primary-config  cf3:/config.cfg
  address        192.168.13.48/20 active
  primary-dns    192.168.1.254
  dns-domain     eng.timetra.com
  autonegotiate

```

```

duplex          full
speed           100
wait            3
persist         off

```

Hit a key within 1 second to change boot parms...

```

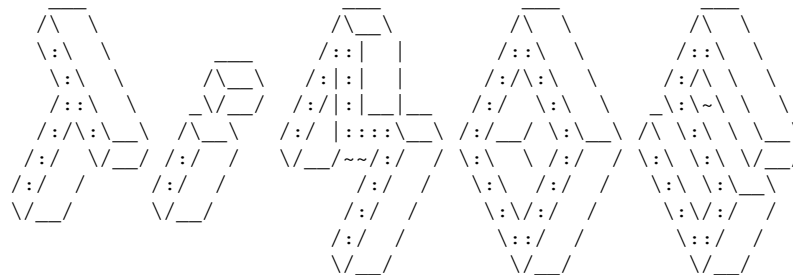
Primary image location: ftp://vxworks:vxw0rks@192.168.15.1/./rel/0.0/I129
Initializing management port tme0 using IP address 192.168.13.48.
Loading image ftp://vxworks:vxw0rks@192.168.15.1/./rel/0.0/I129/both.tim
Version B-0.0.I129, Thurs Jan 13 21:24:57 2011 by builder in /rel0.0/I129/panos/
main
text:(8906865-->21711576) + data:(587508-->5418992)
Executing TiMOS image at 0x2800000

```

```

Total Memory: 512MB Chassis Type: srl Card Type: england_r1
TiMOS-L-14.0.B1-217 boot/i386 Nokia 7750 SR Copyright (c) 2000-2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /rel14.0/b1/B1-217/panos/main

```



```

Time from clock is THU JAN 13 08:39:11 2011 UTC
Attempting to exec configuration file:
'cf3:/config.cfg' ...
System Configuration
Log Configuration
Card Configuration
Port Configuration
Router (Network Side) Configuration
Service Configuration
Router (Service Side) Configuration
Executed 232 lines in 0.0 seconds from file cf3:\config.cfg
ALA-1#

```

5 System Management

5.1 In This Chapter

This chapter provides information about configuring basic system management parameters.

Topics in this chapter include:

- [System Management Parameters](#)
 - [System Information](#)
 - [System Name](#)
 - [System Contact](#)
 - [System Location](#)
 - [System Coordinates](#)
 - [Naming Objects](#)
 - [Naming Objects](#)
 - [Common Language Location Identifier](#)
 - [DNS Security Extensions](#)
 - [System Time](#)
 - [Time Zones](#)
 - [Network Time Protocol \(NTP\)](#)
 - [SNTP Time Synchronization](#)
 - [CRON](#)
- [High Availability](#)
 - [HA Features](#)
 - [Redundancy](#)
 - [Nonstop Forwarding](#)
 - [Nonstop Routing \(NSR\)](#)
 - [CPM Switchover](#)
 - [Synchronization](#)
 - [Synchronization and Redundancy](#)
 - [Synchronous Ethernet](#)
 - [Boot-Env Option](#)

- [Config Option](#)
- [Active and Standby Designations](#)
- [When the Active CPM Goes Offline](#)
- [Persistence](#)
- [Network Synchronization](#)
 - [Central Synchronization Sub-System](#)
 - [7950 XRS-40 Extension Chassis Central Clocks](#)
 - [Synchronization Status Messages \(SSM\)](#)
 - [Synchronous Ethernet](#)
 - [Clock Source Quality Level Definitions](#)
 - [IEEE 1588v2 PTP](#)
- [System-Wide ATM Parameters](#)
- [Link Layer Discovery Protocol \(LLDP\)](#)
- [Ethernet Satellites](#)
 - [Software Repositories for Satellites](#)
 - [Satellite Configuration](#)
 - [Satellite Client Port Association](#)
- [Optical Extension Shelf \(OES\)](#)
- [Administrative Tasks](#)
 - [Configuring the Chassis Mode](#)
 - [Saving Configurations](#)
 - [Specifying Post-Boot Configuration Files](#)
 - [Network Timing](#)
 - [Power Supplies](#)
- [System Router Instances](#)

5.2 System Management Parameters

System management commands allow you to configure basic system management functions such as the system name, the router's location and coordinates, and Common Language Location Identifier (CLLI) code as well as time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) properties, CRON and synchronization properties.

On SR OS routers, it is possible to query the DNS server for IPv6 addresses. By default the DNS names are queried for A-records only (address-preference is IPv4-only). If the address-preference is set to IPv6 first, the DNS server will be queried for AAAA-records first, and if there is no successful reply, then A-records.

5.2.1 System Information

System information components include:

- [System Name](#)
- [System Contact](#)
- [System Location](#)
- [System Coordinates](#)
- [Naming Objects](#)

5.2.1.1 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.

5.2.1.2 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 on how to contact this person. The system contact can be any ASCII-printable text string of up to 80 characters.

5.2.1.3 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.

5.2.1.4 System Coordinates

The system coordinates is the Nokia Chassis MIB `tmnxChassisCoordinates` object. This text string indicates the Global Positioning System (GPS) coordinates of the location of the chassis.

Two-dimensional GPS 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* ranges from 0 to 180 (for latitude) and 0 to 90 for longitude, and 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, examples include:

- 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.

5.2.1.5 Naming Objects

Do not configure named objects with a name that starts with “_tmnx_”, or with “_” in general.

5.2.1.6 Common Language Location Identifier

A CLLI code string for the device is an 11-character standardized geographic identifier that uniquely identifies the geographic location of places and certain 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.

5.2.1.7 DNS Security Extensions

DNS Security (DNSSEC) Extensions are now implemented in the SR OS, allowing operators to configure DNS behavior of the router to evaluate whether the Authenticated Data bit was set in the response received from the recursive name server and to trust the response, or ignore it.

5.2.2 System Time

SR-series 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 SR-series routers OS software has options for local time translation as well as system clock synchronization.

System time parameters include:

- [Time Zones](#)
- [Network Time Protocol \(NTP\)](#)
- [SNTP Time Synchronization](#)
- [CRON](#)

5.2.2.1 Time Zones

Setting a time zone in SR OS allows for times to be displayed in the local time rather than in UTC. The SR OS 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 in length and unique 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 SR OS system-defined time zones are listed in [Table 30](#) which includes both time zones with and without summer time correction.

Table 30 System-defined Time Zones

Acronym	Time Zone Name	UTC Offset
Europe		
GMT	Greenwich Mean Time	UTC

Table 30 System-defined Time Zones (Continued)

Acronym	Time Zone Name	UTC Offset
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
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

Table 30 **System-defined Time Zones (Continued)**

Acronym	Time Zone Name	UTC Offset
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 (e.g., Perth)	UTC +8
ACST	Central Standard Time (e.g., Darwin)	UTC +9.5
AEST	Eastern Standard/Summer Time (e.g., Canberra)	UTC +10

5.2.2.2 Network Time Protocol (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 more importantly they can maintain time in a more synchronized fashion between 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 GPS or atomic clock.

The higher stratum levels are separated from the stratum-1 server over a network path, thus, 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.

SR OS routers will normally operate as a stratum 2 or higher device. The router relies on an external stratum 1 server to source accurate time into the network. However, the SR OS also allows for the use of the local PTP recovered time to be a source into NTP. In this latter case, the local PTP source appears as a stratum 0 server and the SR OS advertises itself as a stratum 1 server. Activation of the PTP source into NTP may impact the network NTP topology.

The following NTP elements are supported:

- **Server mode** — In this mode, the node advertises the ability to act as a clock source for other network elements. In this mode, the node will, by default, transmit NTP packets in NTP version 4 mode.
- **Authentication keys** — Increased security support in carrier and other network has been implemented. Both DES and MD5 authentication are supported as well as multiple keys.
- **Operation in symmetric active mode** — This capability requires that NTP be synchronized with a specific node that is considered more trustworthy or accurate than other nodes carrying NTP in the system. This mode requires that a specific peer is set.
- **Server and peer addressing using IPv6** — Both external servers and external peers may be defined using IPv6 or IPv4 addresses. Other features (such as multicast, broadcast) use IPv4 addressing only.
- **Broadcast or multicast modes** — When operating in these modes, the node will receive or send using either a multicast (default 224.0.1.1) or a broadcast address. Multicast is supported on the MGMT port.
- **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 node, then SNTP transitions to an operationally down state. If NTP is removed from the configuration or shut down, then SNTP resumes an operationally up state.
- **Gradual clock adjustment** — As several applications (such as Service Assurance Agent (SAA)) can use the clock, and if determined that a major (128 ms or more) adjustment needs to be performed, the adjustment is performed by programmatically stepping the clock. If a minor (less than 128 ms) adjustment must be performed, then the adjustment is performed by either speeding up or slowing down the clock.
- **In order to avoid the generation of too many events/trap** the NTP module will rate limit the generation of events/traps to three per second. At that point a single trap will be generated that indicates that event/trap squashing is taking place.

5.2.2.3 SNTP Time Synchronization

For synchronizing the system clock with outside time sources, the SR OS 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 milliseconds 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. External servers may only be specified using IPv4 addresses.

In the SR OS, the SNTP client can be configured for either broadcast or unicast client mode.

5.2.2.4 CRON

The CRON feature supports periodic and date and time-based scheduling in SR OS. CRON can be used, for example, to schedule Service Assurance Agent (SAA) functions. CRON functionality includes the ability to specify scripts that need to be run, when they will be scheduled, including one-time only functionality (one-shot), interval and calendar functions. Scheduled reboots, peer turn ups, service assurance agent tests and more can all be scheduled with CRON, as well as OAM events, such as connectivity checks, or troubleshooting runs.

CRON supports the schedule element. The schedule function configures the type of schedule to run, including one-time only (one-shot), periodic, or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute, and interval (seconds).

5.3 High Availability

This section discusses the high availability (HA) 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 networks.

High availability is an important feature in service provider routing systems. High availability is gaining momentum due to the unprecedented growth of IP 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 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 services which dictates 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, refer to [Synchronization and Redundancy](#).

5.3.1 HA 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 routers. Most of these features only apply to routers with two Control Processor Modules (CPM), currently the 7750 SR-7, SR-12, SR-c12, and ESS-7 models.

- [Redundancy](#)
 - [Software Redundancy](#)
 - [Configuration Redundancy](#)
 - [Component Redundancy](#)

- [Service Redundancy](#)
- [Accounting Configuration Redundancy](#)
- [Nonstop Forwarding](#)
- [Nonstop Routing \(NSR\)](#)
- [CPM Switchover](#)
- [Synchronization](#)
 - [Configuration and boot-env Synchronization](#)
 - [State Database Synchronization](#)

5.3.1.1 Redundancy

The redundancy features enable the duplication of data elements and software functionality to maintain service continuation in case of outages or component failure.

Refer to the *Integrated Services Adapter Guide* for information about redundancy for the Integrated Service Adapter (ISA).

5.3.1.1.1 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 not only throughout the service provider network, but also externally to other connected networks possibly belonging to other service providers. This could affect customers on a broad scale. Presently, there are several software availability features that contribute to the percentage of time that a router is available to process and forward traffic.

To fully appreciate high availability you should realize that all routing protocols specify minimum time intervals in which the peer device must receive an acknowledgment before it disconnects the session.

- OSPF default session timeout is approximately 40 seconds. The timeout intervals are configurable.
- BGP default session timeout is approximately 120 seconds. The timeout intervals are configurable for the 7750 SR and 7950 XRS only.

Therefore, router software has to recover faster than the specified time interval to maintain up time.

5.3.1.1.2 Configuration Redundancy

Features configured on the active device CPM are saved on the standby CPM as well. When the active device CPM fails, these features are brought up on the standby device CPM that takes over the mastership.

Even with modern modular and stable software, the failure of route processor 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 following options are available.

- Warm standby — The router image and configuration is already loaded on the standby route processor. However, the standby could still take a few minutes to become effective since it must first re-initialize connections by bringing up Layer 2 connections and Layer 3 routing protocols and then rebuild routing tables.
- Hot standby — The router image, configuration, and network state is already loaded on the standby and it receives continual updates from the active route processor and the switchover is immediate. However, hot standby affects conventional router performance as more frequent synchronization increases consumption of system resources. Nokia's newer generation service routers address this issue because they already have extra processing built into the system.

5.3.1.1.3 Component Redundancy

Component redundancy is critical to reduce MTTR for the system and primarily consists of the following router features:

- Dual route processor modules — For a highly available architecture, redundant Control Processor Modules (CPM) are essential. The route processing functions of the CPM calculate the most efficient route to an Internet destination and communicate the best path information to peer routers. Rapid information synchronization between the primary and secondary CPMs/CFMs is crucial to minimize recovery time.
- Switch fabric (SFM) redundancy — Failure of a single switch fabric card with little to no loss of traffic.
- Redundant line cards — LAG, ECMP and other techniques to spread traffic over multiple line cards so that a failure of one line card does not impact the services being delivered.
- Redundant power supply — A power module can be removed without impact on traffic.
- Redundant fan — Failure of a fan module 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/from other modules.

Router hardware architecture plays a key role in the availability of the system. The principle router architecture styles are centralized and distributed. In these architectures, both active and standby route processors, I/O modules (IOMs) (also called line cards), fans, and power supplies maintain a low MTTR for the routing system.

However, in a centralized architecture, packet processing and forwarding is performed in a central shared route processor and the individual line cards are relatively simple. The cards rely solely on the route processor for routing and forwarding intelligence and, should the centralized route processor fail, there is greater impact to the system overall, as all routing and packet forwarding will stop.

In a distributed system, the packet forwarding functionality is situated on each line card. Distributing the forwarding engines off the central route processor and positioning one on each line card lowers the impact of route processor failure as the line cards can continue to forward traffic during an outage.

The distributed system is better suited to enable the convergence of business critical services such as real-time voice (VoIP), Video, and VPN applications over IP networks with superior performance and scalability. The centralized architecture can be prone to performance bottleneck issues and limits service offerings through poor scalability which may lead to customer and service SLA violations.

5.3.1.1.4 Service Redundancy

All service-related statistics are kept during a switchover. Services, SDPs, and SAPs will remain up with a minimum loss of forwarded traffic during a CPM switchover.

5.3.1.1.5 Accounting Configuration Redundancy

When there is a switchover and the standby CPM becomes active, the accounting servers will be checked and if they are administratively up and capable of coming online (media present, etc.), the standby will be brought online and new accounting files will be created at that point. Users must manually copy the accounting records from the failed CPM.

5.3.1.2 Nonstop Forwarding

In a control plane failure or a forced switchover event, the router continues to forward packets using the existing stale forwarding information. Nonstop forwarding requires clean control plane and data plane separation. Usually the forwarding information is distributed to the IOMs, XCMs and XMA.

Nonstop forwarding is used to notify peer routers to continue forwarding and receiving packets, even if the route processor (control plane) is not working or is in a switch-over state. Nonstop forwarding requires clean control plane and data plane separation and usually the forwarding information is distributed to the line cards. This method of availability has both advantages and disadvantages. Nonstop forwarding continues to forward packets using the existing stale forwarding information during a failure. This may cause routing loops and black holes, and also requires that surrounding routers adhere to separate extension standards for each protocol. Every router vendor must support protocol extensions for interoperability.

5.3.1.3 Nonstop Routing (NSR)

With NSR on the SR-series router devices, 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 SR-series routers supports all routing protocols. NSR makes it possible to keep the existing sessions (BGP, LDP, OSPF, etc.) during a CPM switchover, including support for MPLS signaling protocols. Peers will not see any change.

Protocol extensions are not required. There are no interoperability issues and there is no need to define protocol extensions for every protocol. Unlike nonstop forwarding and graceful restart, the forwarding information in NSR is always up to date, which eliminates possible blackholes or forwarding loops.

Traditionally, addressing high availability issues have been patched through non-stop forwarding solutions. With the implementation of NSR, these limitations are overcome by delivering an intelligent hitless failover solution. This enables a carrier-class foundation for transparent networks, required to support business IP services backed by stringent SLAs. This level of high availability poses a major issue for conventional routers whose architectural design limits or prevents them from implementing NSR.

5.3.1.4 CPM Switchover

During a switchover, system control and routing protocol execution are transferred from the active to the standby CPM.

An automatic switchover may occur under the following conditions:

- A fault condition that causes the active CPM to crash or reboot.
- The active CPM is declared down (not responding).
- Online removal of the active CPM.

A manual switchover can occur under the following conditions:

- To force a switchover from an active CPM to a standby, use the `admin redundancy force-switchover` command. You can configure a batch file that executes after failover by using the **config system switchover-exec** CLI command.

5.3.1.5 Synchronization

Synchronization between the CPMs includes the following:

- [Configuration and boot-env Synchronization](#)
- [State Database Synchronization](#)

5.3.1.5.1 Configuration and boot-env Synchronization

Configuration and boot-env synchronization are supported in **admin>redundancy>synchronize** and **config>redundancy>synchronize** contexts.

5.3.1.5.2 State Database Synchronization

If a new standby CPM is inserted into the system, it synchronizes with the active CPM upon a successful boot process.

If the standby CPM is rebooted, it synchronizes with the active CPM upon a successful boot process.

When configuration or state changes occur, an incremental synchronization is conducted from the active CPM to the standby CPM.

If the synchronization fails, the standby does not reboot automatically. The **show redundancy synchronization** command displays synchronization output information.

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

5.4 Synchronization and Redundancy

SR-series routers supporting redundancy use a 1:1 redundancy scheme. Redundancy methods facilitate system synchronization between the active and standby Control Processor Modules (CPMs) so they maintain identical operational parameters to prevent inconsistencies in the event of a CPM 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 CPM file system are mirrored in the standby CPM file system.

Although software configurations and images can be copied or downloaded from remote locations, synchronization can only occur locally between compact flash drives (cf1:, cf2:, and cf3:).

Synchronization can occur either:

- Automatically — Automatic synchronization is disabled by default. To enable automatic synchronization, the **config>redundancy>synchronization** 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 and when an **admin>save** command is entered with no filename specified.

- Manually — To execute synchronization manually, the **admin>redundancy>synchronization** 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.

```
A:ALA-12>admin>redundancy# synchronize config
Syncing configuration.....

Syncing configuration.....Completed.
A:ALA-12#
```

5.4.1 Active and Standby Designations

Typically, the first Switch Fabric (SF)/CPM card installed in a redundant SR-series router chassis assumes the role as active, regardless of being inserted in Slot A or B. The next CPM installed in the same chassis then assumes the role as the standby CPM. If two CPM are inserted simultaneously (or almost simultaneously) and are booting at the same time, then preference is given to the CPM installed in Slot A.

If only one CPM is installed in a redundant router device, then it becomes the active CPM regardless of the slot it is installed in.

The active and standby designations can be visually determined by LEDs on the CPM/CFM/CCM faceplate. Please see the appropriate platform Installation Guide for LED indicator details.

The following output shows that the CPM installed in Slot A is acting as the active CPM and the CPM installed in Slot B is acting as the standby.

The following is an example of the 7950 XRS output:

```
*A:7950 XRS-20# show card
=====
Card Summary
=====
Slot   Provisioned Type           Admin Operational  Comments
      Equipped Type (if different) State State
-----
1      xcm-x20                    up    provisioned
A      cpm-x20                    up    up/active
```

```
B          cpm-x20                                up    up/standby
=====
```

The following console message displays when a CPM boots, sees an active CPM, and becomes the standby CPM:

```
...
Slot A contains the Active CPM
This CPM (Slot B) is the Standby CPM
```

5.4.2 When the Active CPM Goes Offline

When an active CPM goes offline (due to reboot, removal, or failure), the standby CPM takes control without rebooting or initializing itself. It is assumed that the CPMs are synchronized, therefore, there is no delay in operability. When the CPM that went offline boots and then comes back online, it becomes the standby CPM.

When the standby CPM comes online, the following output is shown:

```
Active CPM in Slot A has stopped
Slot B is now active CPM

Attempting to exec configuration file:
'cf3:/config.cfg' ...

...

Executed 49,588 lines in 8.0 seconds from file cf3:\config.cfg
```

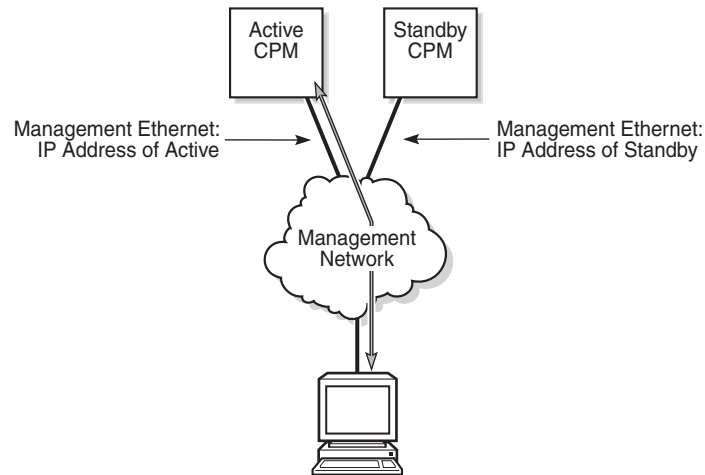
5.4.3 OOB Management Ethernet Port Redundancy

The SR OS platform provides a resilient out-of-band (OOB) management Ethernet redundancy mode for system management.

When the management Ethernet port is down on the active CPM, the OOB Ethernet redundancy feature allows the active CPM to use the management Ethernet port of the standby CPM, as shown in [Figure 11](#) and [Figure 12](#).

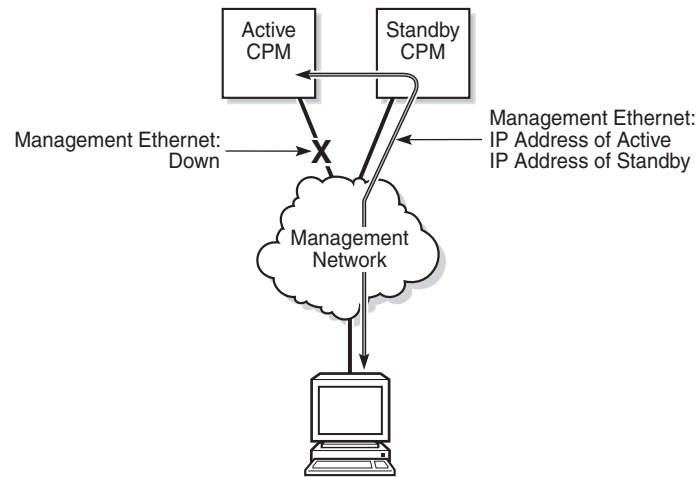
OOB management Ethernet port redundancy is enabled using the **configure>redundancy>mgmt-ethernet-redundancy** command.

Figure 11 Management Ethernet: Normal Mode



25169

Figure 12 Management Ethernet: Redundancy Mode



25168

5.4.4 Persistence

The persistence feature on the 7750 SR allows information learned through DHCP snooping across reboots to be kept. This information can include data such as the IP address, MAC binding information, lease length information, and ingress sap information (required for VPLS snooping to identify the ingress interface). This information is referred to as the DHCP lease-state information.

When a DHCP message is snooped, there are steps that make the data persistent in a system with dual CPMs. In systems with only one CPM, only Step 1 applies. In systems with dual CPMs, all steps apply.

1. When a DHCP ACK is received from a DHCP server, the entry information is written to the active CPM Compact Flash. If writing was successful, the ACK is forwarded to the DHCP client. If persistency fails completely (bad cflash), a trap is generated indicating that persistency can no longer be guaranteed. If the complete persistency system fails the DHCP ACKs are still forwarded to the DHCP clients. Only during small persistency interruptions or in overload conditions of the Compact Flash, DHCP ACKs may get dropped and not forwarded to the DHCP clients.
2. DHCP message information is sent to the standby CPM and also there the DHCP information is logged on the Compact Flash. If persistency fails on the standby also, a trap is generated.

5.4.4.1 Dynamic Data Persistency (DDP) Access Optimization for DHCP Leases

A high rate of DHCP renewals can create a load on the compact flash file system when subscriber management and/or DHCP server persistence is enabled. To optimize the access to the Dynamic Data Persistency (DDP) files on the compact flash, a lease-time threshold can be specified that controls the eligibility of a DHCP lease for persistency updates when no other data other than the lease expiry time is to be updated.

```
configure
  system
    persistence
      subscriber-mgmt
        location cf2:
      exit
      dhcp-server
        location cf2:
      exit
      options
        dhcp-leasetime-threshold [days <days>] [hrs <hours>]
```

```
[min <minutes>] [sec <seconds>]
    exit
    exit
    exit
```

When the offered lease time of the DHCP lease is less than the configured threshold, the lease is flagged to skip persistency updates and will be installed with its full lease time upon a persistency recovery after a reboot.

The **dhcp-lease-time-threshold** command controls persistency updates for:

- DHCPv4 and DHCPv6 leases for a DHCP relay or proxy (enabled with **persistence subscriber-mgmt**)
- DHCPv4 leases for DHCP snooping in a VPLS service (enabled with **persistence subscriber-mgmt**)
- DHCPv4 and DHCPv6 leases for a DHCP server (enabled with **persistence dhcp-server**)

To check if a DHCP relay or proxy lease is flagged to skip persistency updates, use the **tools dump persistence submgt record record-key** CLI command. When flagged to skip persistency updates, the persistency record output will include “Skip Persistency Updates: true”.

To check if a DHCP server lease is flagged to skip persistency updates, use the **tools dump persistence dhcp-server record record-key** CLI command. When flagged to skip persistency updates, the persistency record output will include “lease mode : LT” (LT = Lease Time) and a “lease time : ...” field. When not flagged to skip persistency updates, the persistency record output will include “lease mode : ET” (ET = Expiry Time) and an “expires : ...” field.

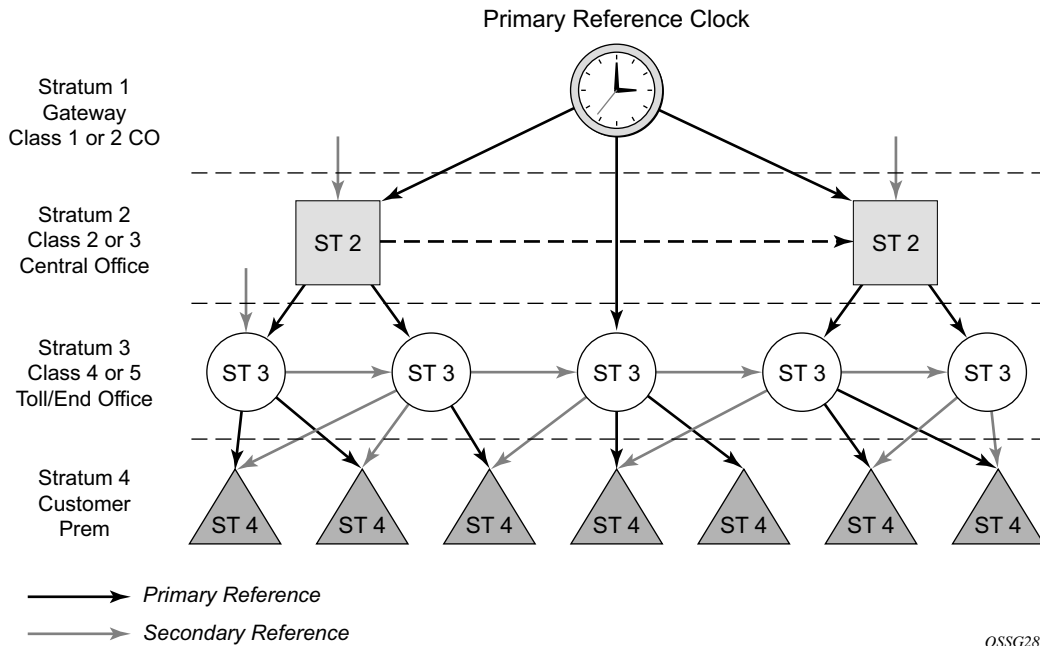
5.5 Network Synchronization

This section describes network synchronization capabilities available on SR OS platforms. These capabilities involve multiple approaches to network timing; namely SDH/SONET, Synchronous Ethernet, BITS, and Adaptive clocking and a Precision Time Protocol (PTP) IEEE 1588v2. These features address barriers to entry by:

- Providing synchronization quality required by the mobile space; such as radio operations and circuit emulation services (CES) transport.
- Augmenting and potentially replacing the existing (SONET/SDH) timing infrastructure and delivering high quality network timing for time sensitive applications in the wireline space.

Network synchronization is commonly distributed in a hierarchical master-slave topology at the physical layer as shown in [Figure 13](#).

Figure 13 Conventional Network Timing Architecture (North American Nomenclature)



The architecture shown in [Figure 13](#) provides the following benefits:

- Limits the need for high quality clocks at each network element and only requires that they reliably replicate input to remain traceable to its reference.
- Uses reliable physical media to provide transport of the timing signal; it doesn't consume any bandwidth and requires limited additional processing.

The synchronization network is designed so a clock always receives timing from a clock of equal or higher stratum or quality level. This ensures that if an upstream clock has a fault condition (for example, loses its reference and enters a holdover or free-run state) and begins to drift in frequency, the downstream clock will be able to follow it. For greater reliability and robustness, most offices and nodes have at least two synchronization references that can be selected in priority order (such as primary and secondary).

Further levels of resiliency can be provided by designing a capability in the node clock that will operate within prescribed network performance specifications without any reference for a specified time-frame. A clock operating in this mode is said to hold the last known state over (or holdover) until the reference lock is once again achieved. Each level in the timing hierarchy is associated with minimum levels of network performance.

Each synchronization capable port can be independently configured to transmit data using the node reference timing or loop timing. In addition, some TDM channels can use adaptive timing.

Transmission of a reference clock through a chain of Ethernet equipment requires that all equipment supports Synchronous Ethernet. A single piece of equipment that is not capable of performing Synchronous Ethernet breaks the chain. Ethernet frames will still get through but downstream devices should not use the recovered line timing as it will not be traceable to an acceptable stratum source.

5.5.1 Central Synchronization Sub-System

The timing subsystem for the platforms has a central clock located on the CPM (motherboard). The timing subsystem performs many of the duties of the network element clock as defined by Telcordia (GR-1244-CORE) and ITU-T G.781.

The system can select from up to three (7950 XRS) or four (7450 ESS and 7750 SR) timing inputs to train the local oscillator. The priority order of these references must be specified. This is a simple ordered list of inputs: {bits, ref1, ref2, ptp}. The CPM clock output shall have the ability to drive the clocking for all line cards in the system. The routers support selection of the node reference using Quality Level (QL) indications. See Figure 14 for a description of the synchronization selection process for the CPM clock.


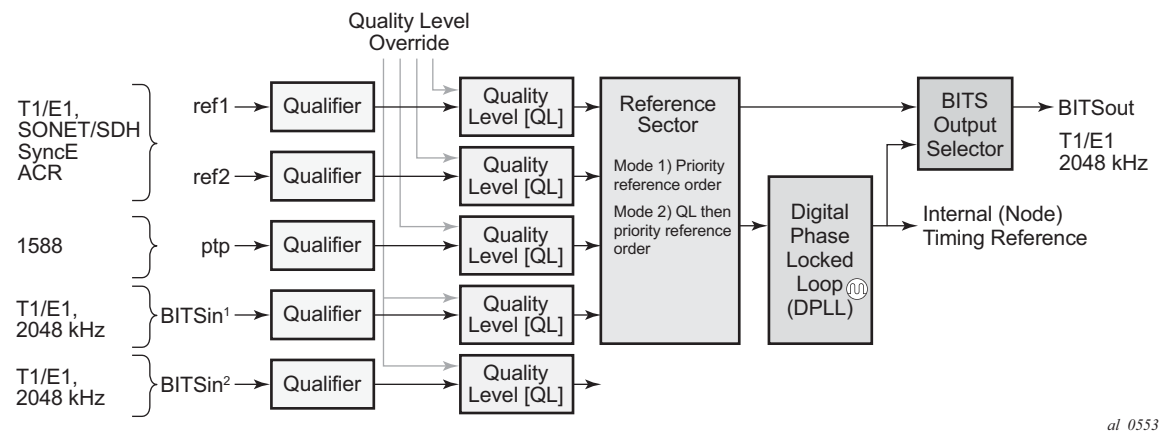
 **Note:** Not all signals are available on all platforms.

Figure 14 CPM Clock Synchronization Reference Selection



al_0553

The recovered clock will be able to derive its timing from any of the following:

- OC3/STM1, OC12/STM4, OC48/STM16, OC192/STM64 ports (7450 ESS and 7750 SR only)
- T1/E1 CES channel (adaptive clocking) (7750 SR only)
- Synchronous Ethernet ports
- T1/E1 port (7750 SR only)
- BITS port on a Channelized OC3/STM1 CES CMA (7750 SR-c12 only)
- BITS port on the CPM, CFM, or CCM module
- 10GE ports in WAN PHY mode
- IEEE 1588v2 slave port (PTP) (7450 ESS and 7750 SR only)

The BITS ports accept T1 or E1 signal formats. Some hardware also supports the 2048 kHz signal format. The format must be common between all BITSin and BITSout ports.

All settings of the signal characteristics for the BITS input apply to both ports. When the active CPM considers the BITS input as a possible reference, it will consider first the BITS input port on the active CPM or CCM followed by the BITS input port on the standby CPM or CCM in that relative priority order. This relative priority order is in addition to the user-definable **ref-order**. For example, a **ref-order** of **bits ref1 ref2** would actually be BITS in (active CPM or CCM), followed by BITS in (standby CPM or CPM), followed by ref1, followed by ref2. When **ql-selection** is enabled, the QL of each BITS input port is viewed independently. The higher QL source is chosen.

The 7750 SR-c4 platform has a CFM, there are two BITS input ports and two BITS output ports on this one module. These two ports are provided for BITS redundancy for the chassis. All settings of the signal characteristics for the BITS input applies to both ports. This includes the ql-override setting. When the CFM considers the BITS input as a possible reference, it will consider first the BITS input port “bits1” followed the BITS input port “bits2” in that relative priority order. This relative priority order is in addition to the user definable **ref-order**. For example, a **ref-order** of **bits ref1 ref2** would actually be “bits1”, followed by “bits2”, followed by ref1, followed by ref2. When **ql-selection** is enabled, the QL of each BITS input port is viewed independently. The higher QL source is chosen.

The BITS output ports can be configured to provided either the unfiltered recovered line clock from a line card port or the output of the central clock. The first case would be used if the port was connected to deliver an input reference directly to dedicated timing device in the facility (BITS or SASE device). The second case would be used to test the quality of the clocking used by the router.

When QL selection mode is disabled, then the reversion setting controls when the central clock can re-select a previously failed reference.

The [Table 31](#) shows the selection followed for two reference in both revertive and non-revertive modes:

Table 31 **Revertive, non-Revertive Timing Reference Switching Operation**

Status of Reference A	Status of Reference B	Active Reference Non-revertive Case	Active Reference Revertive Case
OK	OK	A	A
Failed	OK	B	B
OK	OK	B	A
OK	Failed	A	A
OK	OK	A	A
Failed	Failed	holdover	holdover
OK	Failed	A	A
Failed	Failed	holdover	holdover
Failed	OK	B	B
Failed	Failed	holdover	holdover
OK	OK	A or B	A

5.5.2 7950 XRS-40 Extension Chassis Central Clocks

The central clock architecture described above applies to each chassis of the 7950 XRS-40. There is a central clock located on each of the CPMs present in the extension chassis. However, there is no configuration for the central clocks on the CPMs of the extension chassis. The central clocks only use the BITS input ports of the extension chassis for their input reference. It is assumed that the quality of the reference provided into the BITS input ports of the extension chassis CPMs is equal to the quality of the Master chassis central clocks. See the installation guide for appropriate physical cabling to support this architecture.

5.5.3 Synchronization Status Messages (SSM)

SSM provides a mechanism to allow the synchronization distribution network to both determine the quality level of the clock sourcing a given synchronization trail and to allow a network element to select the best of multiple input synchronization trails. Synchronization Status messages have been defined for various transport protocols including SONET/SDH, T1/E1, and Synchronous Ethernet, for interaction with office clocks, such as BITS or SSUs and embedded network element clocks.

SSM allows equipment to autonomously provision and reconfigure (by reference switching) their synchronization references, while helping to avoid the creation of timing loops. These messages are particularly useful to allow synchronization reconfigurations when timing is distributed in both directions around a ring.

The following sections provide details about the SSM message functionality for different signal types. These functions apply to all platforms that support the given signal type.

5.5.3.1 DS1 Signals

DS1 signals can carry an indication of the quality level of the source generating the timing information using the SSM transported within the 1544 Kbit/s signal's Extended Super Frame (ESF) Data Link (DL) as specified in Recommendation G.704. No such provision is extended to SF formatted DS1 signals.

The format of the data link messages in ESF frame format is "0xxx xxx0 1111 1111", transmitted rightmost bit first. The six bits denoted "xxx xxx" contain the actual message; some of these messages are reserved for synchronization messaging. It takes 32 frames (such as 4 ms) to transmit all 16 bits of a complete DL.

5.5.3.2 E1 Signals

E1 signals can carry an indication of the quality level of the source generating the timing information using the SSM as specified in Recommendation G.704.

One of the Sa4 to Sa8 bits, (the actual Sa bit is for operator selection), is allocated for Synchronization Status Messages. To prevent ambiguities in pattern recognition, it is necessary to align the first bit (San1) with frame 1 of a G.704 E1 multi-frame.

The numbering of the San (n = 4, 5, 6, 7, 8) bits. A San bit is organized as a 4-bit nibble San1 to San4. San1 is the most significant bit; San4 is the least significant bit.

The message set in San1 to San4 is a copy of the set defined in SDH bits 5 to 8 of byte S1.

5.5.3.3 SONET/SDH Signals

The SSM of SDH and SONET interfaces is carried in the S1 byte of the frame overhead. Each frame contains the four bit value of the QL.

5.5.3.4 DS3/E3

DS3/E3 signals are not required to be synchronous. However, it is acceptable for their clocking to be generated from a synchronization source. The 7750 SR and the 7450 ESS permit E3/DS3 physical ports to be specified as a central clock input reference.

DS3/E3 signals do not support an SSM channel. QL-override should be used for these ports if ql-selection is enabled

5.5.4 Synchronous Ethernet

Traditionally, Ethernet-based networks employ the physical layer transmitter clock to be derived from an inexpensive +/-100ppm crystal oscillator and the receiver locks onto it. There is no need for long term frequency stability because the data is packetized and can be buffered. For the same reason there is no need for consistency between the frequencies of different links. However, you can derive the physical layer transmitter clock from a high quality frequency reference by replacing the crystal with a frequency source traceable to a primary reference clock. This would not effect the operation of any of the Ethernet layers, for which this change would be transparent. The receiver at the far end of the link would lock onto the physical layer clock of the received signal, and thus itself gain access to a highly accurate and stable frequency reference. Then, in a manner analogous to conventional hierarchical master-slave network synchronization, this receiver could lock the transmission clock of its other ports to this frequency reference and a fully time synchronous network could be established.

The advantage of using Synchronous Ethernet, compared with methods that rely on sending timing information in packets over an unclocked physical layer, is that it is not influenced by impairments introduced by the higher levels of the networking technology (packet loss, packet delay variation). Hence, the frequency accuracy and stability may be expected to exceed those of networks with unsynchronized physical layers.

Synchronous Ethernet allows operators to gracefully integrate existing systems and future deployments into conventional industry-standard synchronization hierarchy. The concept behind synchronous Ethernet is analogous to SONET/SDH system timing capabilities. It allows the operator to select any (optical) Ethernet port as a candidate timing reference. The recovered timing from this port will then be used to time the system (for example, the CPM will lock to this provisioned reference selection). The operator then could ensure that any of system output would be locked to a stable traceable frequency source.

If the port is a fixed copper Ethernet port and in 1000BASE-T mode of operation, there is a dependency on the 802.3 link timing for the Synchronous Ethernet functionality (refer to ITU-T G.8262). The 802.3 link Master-Slave timing states must align with the desired direction of Synchronous Ethernet timing flow. When a fixed copper Ethernet port is specified as an input reference for the node or when it is removed as an input reference for the node, an 802.3 link auto-negotiation is triggered to ensure the link timing aligns properly.

The SSM of Synchronous Ethernet uses an Ethernet OAM PDU that uses the slow protocol subtype. For a complete description of the format and processing see ITU-T G.8264

5.5.5 Clock Source Quality Level Definitions

The following clock source quality levels have been identified for the purpose of tracking network timing flow. These levels make up all of the defined network deployment options given in Recommendation G.803 and G.781. The Option I network is a network developed on the original European SDH model; whereas, the Option II network is a network developed on the North American SONET model.

In addition to the QL values received over SSM of an interface, the standards also define additional codes for internal use. These include the following:

- QL INVx is generated internally by the system if and when an unallocated SSM value is received, where x represents the binary value of this SSM. All of these independent values are assigned as the singled value of QL-INVALID.
- QL FAILED is generated internally by the system if and when the terminated network synchronization distribution trail is in the signal fail state.

There is also an internal quality level of QL-UNKNOWN. This is used to differentiate from a received QL-STU code but is equivalent for the purposes of QL selection.

Table 32 Synchronization Message Coding and Source Priorities — SSM Received

SSM value received on port				
SDH interface SyncE interface in SDH mode	SONET Interface SyncE interface in SONET mode	E1 interface	T1 interface (ESF)	Internal Relative Quality Level
0010 (prc)	0001 (prs)	0010 (prc)	00000100 11111111 (prs)	1 - Best quality
	0000 (stu)		00001000 11111111 (stu)	2
	0111 (st2)		00001100 11111111 (ST2)	3
0100 (ssua)	0100 (tnc)	0100 (ssua)	01111000 11111111 (TNC)	4
	1101 (st3e)		01111100 11111111 (ST3E)	5
1000 (ssub)		1000 (ssub)		6
	1010 (st3/eec2)		00010000 11111111 (ST3)	7
1011 (sec/eec1)		1011 (sec)		8 - Lowest quality qualified in QL- enabled mode
	1100 (smc)		00100010 11111111 (smc)	9
			00101000 11111111 (st4)	10
	1110 (pno)		01000000 11111111 (pno)	11
1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)	12
Any other	Any other	Any other	N/A	13- QL_INVALID
				14- QL-FAILED
				15 - QL-UNC

Table 33 Synchronization Message Coding and Source Priorities — SSM Transmitted

SSM values to be transmitted by interface of type				
Internal Relative Quality Level	SDH interface SyncE interface in SDH mode	SONET Interface SyncE interface in SONET mode	E1 interface	T1 interface (ESF)
1 - Best quality	0010 (prc)	0001 (PRS)	0010 (prc)	00000100 11111111 (PRS)
2	0100 (ssua)	0000 (stu)	0100 (ssua)	00001000 11111111 (stu)
3	0100 (ssua)	0111 (st2)	0100 (ssua)	00001100 11111111 (st2)
4	0100 (ssua)	0100 (tnc)	0100 (ssua)	01111000 11111111 (tnc)
5	1000 (ssub)	1101 (st3e)	1000 (ssub)	01111100 11111111 (st3e)
6	1000 (ssub)	1010 (st3/eec2)	1000 (ssub)	00010000 11111111 (st3)
7	1011 (sec/eec1)	1010 (st3/eec2)	1011 (sec)	00010000 11111111 (st3)
8 - Lowest quality qualified in QL- enabled mode	1011 (sec/ eec1)	1100 (smc)	1011 (sec)	00100010 11111111 (smc)
9	1111 (dnu)	1100 (smc)	1111 (dnu)	00100010 11111111 (smc)
10	1111 (dnu)	1111 (dus)	1111 dnu	00101000 11111111 (st4)
11	1111 (dnu)	1110 (pno)	1111 (dnu)	01000000 11111111 (pno)
12	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
13- QL_INVALID	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
14- QL-FAILED	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
15 - QL-UNC	1011 (sec/eec1)	1010 (st3/eec2)	1011 (sec)	00010000 11111111 (st3)



Note: When the internal Quality level is in the range of 9 through 14, the output codes shown in [Table 33](#), will only appear if QL selection is disabled. If ql-selection is enabled, then all of these internal states are changed to internal state 15 (Holdover) and the ssm value generated will reflect the holdover quality of the internal clock.

5.5.6 IEEE 1588v2 PTP

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard 1588 PTP 2008. Support for PTP is dependent on both platform and software release; check the release notes for applicability.

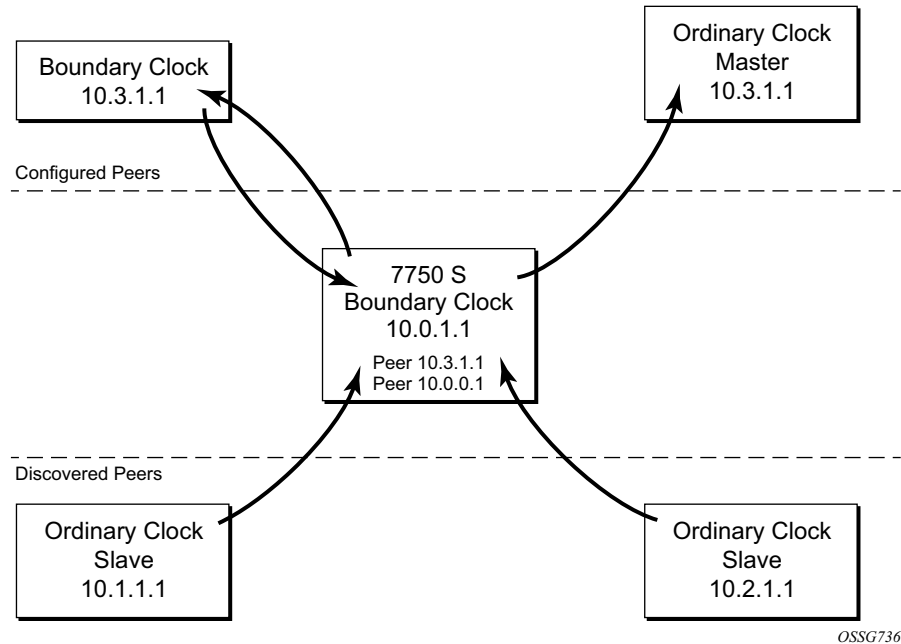
PTP may be deployed as an alternative timing-over-packet option to ACR. PTP provides the capability to synchronize network elements to a Stratum-1 clock or primary reference clock (PRC) traceable frequency source over a network that may or may not be PTP-aware. PTP has several advantages over ACR. It is a standards-based protocol, has lower bandwidth requirements, can transport both frequency and time, and can potentially provide better performance.

The PTP functionality has dependencies on hardware components in the applicable platform. Refer to the relevant release notes for details.

Support is provided for an ordinary clock in slave or master mode or a boundary clock. When configured as an ordinary clock master, PTP can only be used for the distribution of a frequency reference, not a time reference. The boundary clock and ordinary clock slave can be used for both frequency and time distribution.

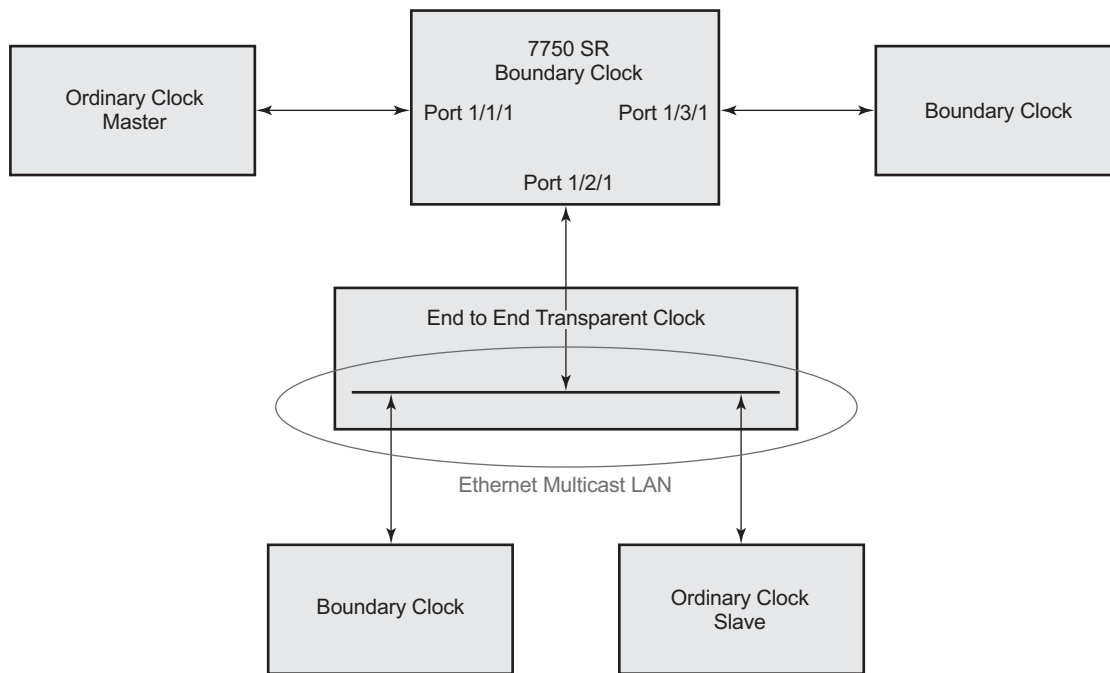
The ordinary clock master, ordinary clock slave, and boundary clock communicate with neighboring IEEE 1588v2 clocks. These neighbor clocks can be ordinary clock masters, ordinary clock slaves, or boundary clocks. The communication can be based on either unicast IPv4 sessions transported through IP interfaces or multicast Ethernet transported through Ethernet ports.

For the unicast IP sessions, the external clocks are labeled 'peers'. There are two types of peers: configured and discovered. An ordinary clock slave or a boundary clock should have configured peers for each PTP neighbor clock from which it might accept synchronization information. The router initiates unicast sessions with all configured peers. An ordinary clock master or boundary clock will accept unicast session requests from external peers. If the peer is not a configured peer, then it is considered a discovered peer. An ordinary clock master or boundary clock can deliver synchronization information toward discovered peers. [Figure 15](#) shows the relationship of various neighbor clocks using unicast IP sessions to communicate with a 7750 SR configured as a boundary clock with two configured peers.

Figure 15 Peer Clocks

For multicast Ethernet operation, the router shall listen for and transmit PTP messages using the configured multicast MAC address. Neighbor clocks are discovered via the reception of messages through an enabled Ethernet port. An ordinary clock master, ordinary clock slave, and a boundary clock support more than one neighbor PTP clock connecting into a single port. This might be encountered with the deployment of an Ethernet multicast LAN segment between the local clock and the neighbor PTP ports using an End to end transparent clock or an Ethernet switch. The Ethernet switch is not recommended due to the introduction of PDV and the potential degradation of performance but it can be used if appropriate to the application. [Figure 16](#) shows the relationship of various neighbor clocks using multicast Ethernet sessions to a 7750 SR configured as a boundary clock. The 7750 SR has three ports configured for multicast Ethernet communications. Port 1/2/1 of the 7750 SR shows a connection where there are two neighbor clocks connecting to one port of the 7750 SR through an end-to-end transparent clock.

Figure 16 Ethernet Multicast Ports



al_0527

The ordinary clock master, ordinary clock slave, and boundary clock allow for PTP operation over both unicast IPv4 and multicast Ethernet at the same time.

The IEEE 1588v2 standard includes the concept of PTP profiles. These profiles are defined by industry groups or standards bodies that define how IEEE 1588v2 is to be used for a particular application.

Currently, three profiles are supported:

- IEEE 1588v2 default profile
- ITU-T Telecom profile for frequency (G.8265.1)
- ITU-T Telecom profile for time with full timing support (G.8275.1)

When an ordinary clock slave or a boundary clock receive *Announce* messages from one or more configured peers or multicast neighbors, it executes a Best Master Clock Algorithm (BMCA) to determine the state of communication between itself and the peers. The system uses the BMCA to create a hierarchical topology allowing the flow of synchronization information from the best source (the Grandmaster clock) out through the network to all boundary and slave clocks. Each profile has a dedicated BMCA.

If the **profile** setting for the clock is `ieee1588-2008`, the precedence order for the best master selection algorithm is as follows:

- priority1
- clock class
- clock accuracy
- PTP variance (offsetScaledLogVariance)
- priority2
- clock identity
- steps removed from the grandmaster

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as follows:

Table 34 Local Clock Parameters When Profile is set to ieee1588-2008

Parameter	Value
clockIdentity	Chassis MAC address following the guidelines of 7.5.2.2.2 of IEEE 1588
clockClass	13 — local clock configured as ordinary clock master and is locked to an external reference 14 — local clock configured as ordinary clock master and in holdover after having been locked to an external source 248 — local clock configured as ordinary clock master and is in free run or the router is configured as a boundary clock 255 — local clock configured as ordinary clock slave
clockAccuracy	FE — unknown
offsetScaledLogVariance	FFFF — not computed

If the **profile** setting for the clock is g8265dot1-2010, the precedence order for the best master selection algorithm is:

- clock class
- priority

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as follows:

Table 35 Local Clock Parameters When Profile is set to: itu-telecom-freq

Parameter	Value
clockClass	80-110 — value corresponding to the QL out of the central clock as per Table 1/G.8265.1 255 — the clock is configured as ordinary clock slave

The g8265dot1-2010 profile is for use in an environment with only ordinary clock masters and slaves for frequency distribution.

If the **profile** setting for the clock is g8275dot1-2014, the precedence order for the best master selection algorithm is very similar to that used with the default profile. It ignores the **priority1** parameter, includes a **localPriority** parameter and includes the ability to force a port to never enter slave state (**master-only**). The precedence is as follows:

- clock class
- clock accuracy
- PTP variance (offsetScaledLogVariance)
- priority2
- localPriority
- clock identity
- steps removed from the grandmaster

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as follows:

Table 36 Local Clock Parameters When Profile is set to: g8275dot1-2014

Parameter	Value
clockIdentity	Chassis MAC address following the guidelines of 7.5.2.2.2 of IEEE 1588
clockClass	165 — local clock configured to a boundary clock and the boundary clock was previously locked to a grandmaster with a clock class of 6 248 — local clock configured as boundary clock 255 — local clock configured as ordinary clock slave
clockAccuracy	FE — unknown
offsetScaledLogVariance	FFFF — not computed

There is a limit on the number of external PTP clocks to which the ordinary clock slave or boundary clock will request unicast service (# configured peers) and also a limit to the number of external PTP clocks to which the ordinary clock master or boundary clock will grant unicast service (# discovered peers). An association where the boundary clock has a symmetric relationship with another boundary clock (i.e. they both have the other as a configured peer) will consume a request and a grant unicast service in each router.

The number of configured Ethernet ports is not restricted.

There are limits to the maximum transmitted and received event message rates supported in the router. Each unicast IP service established will consume a portion of one of the unicast message limits. Once either limit is reached, additional unicast service requests will be refused by sending a grant response with zero in the duration field.

Please refer to the scaling guide for the appropriate release for the specific unicast message limits related to PTP.

Multicast messages are not considered when validating the unicast message limit. When multicast messaging on Ethernet ports is enabled, the PTP load needs to be monitored to ensure the load does not exceed the capabilities. There are several commands that can be used for this monitoring:

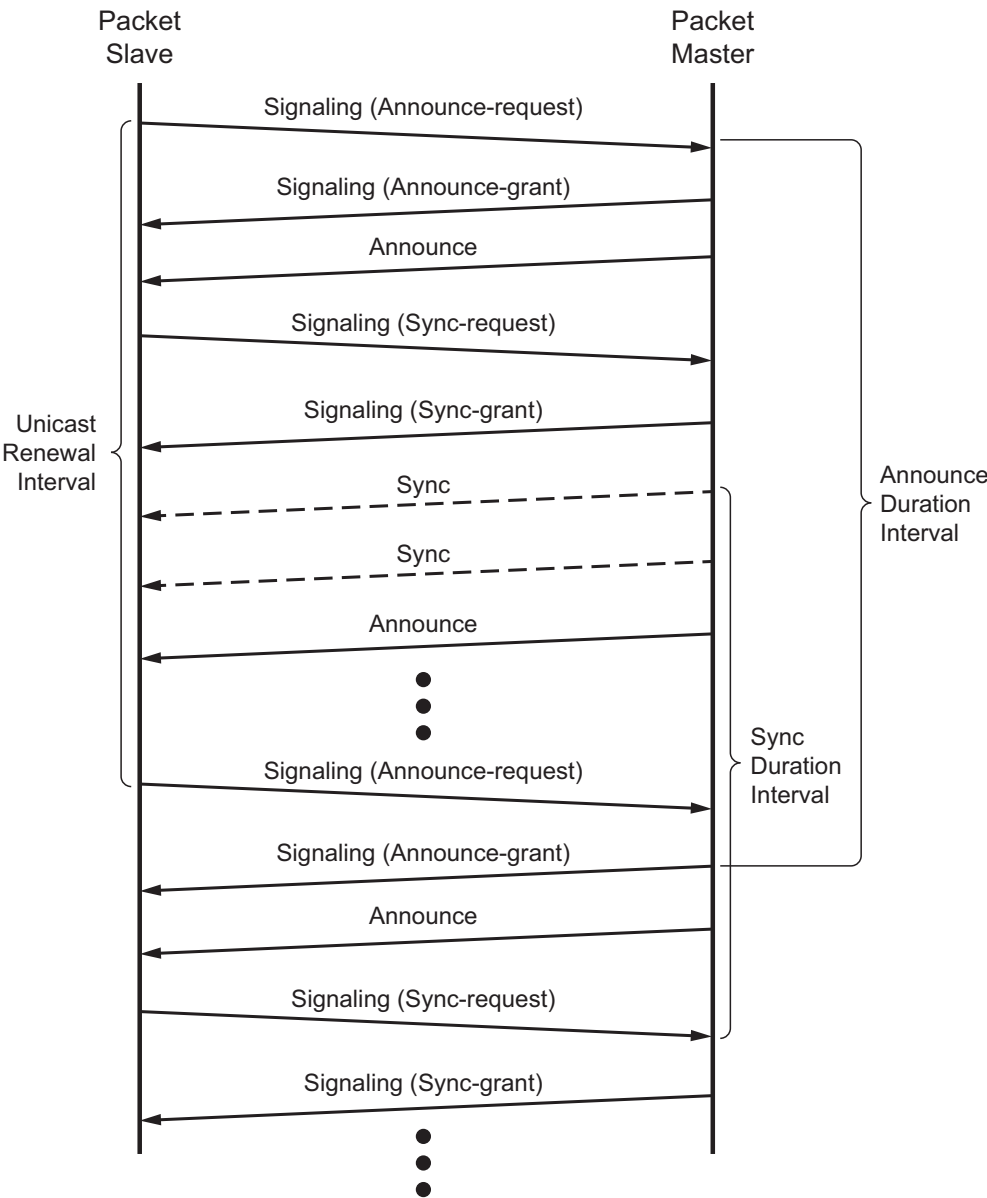
- 'show system cpu' will identify the load of the PTP software process. If the "capacity usage" reaches 100%, the PTP software process on the router is at its limit of transmitting and/or receiving PTP packets.

Because the user cannot control the amount of PTP messages being received over the Ethernet ports, the statistics commands can be used to identify the source of the message load:

- 'show system ptp statistics' has aggregate packet rates
- 'show system ptp port' and 'show system ptp port port-id [detail]' display received packet rates

Figure 17 shows the unicast negotiation procedure performed between a slave and a peer clock that is selected to be the master clock. The slave clock will request Announce messages from all peer clocks but only request Sync and Delay_Resp messages from the clock selected to be the master clock.

Figure 17 Messaging Sequence Between the PTP Slave Clock and PTP Master Clock



OSSG666

5.5.6.1 PTP Clock Synchronization

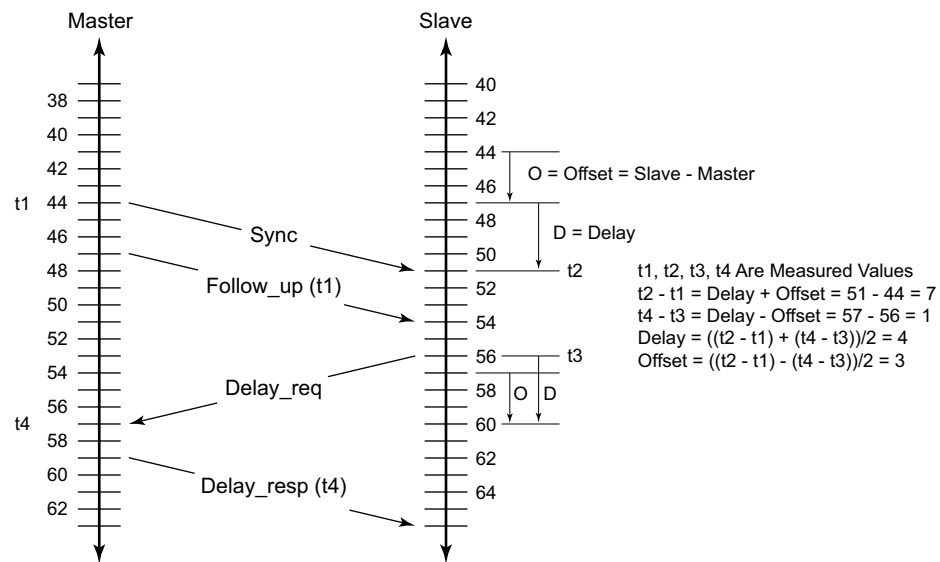
The IEEE 1588v2 standard allows for synchronization of the frequency and time from a master clock to one or more slave clocks over a packet stream. This packet-based synchronization can be over unicast UDP/IPv4 or multicast Ethernet.

As part of the basic synchronization timing computation, a number of event messages are defined for synchronization messaging between the PTP slave port and PTP master port. 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. Ordinary clock master and boundary clock master ports use one-step operation; ordinary clock slave and boundary clock slave ports can accept messages from either one-step or two-step operation master ports.

The IEEE 1588v2 standard includes a mechanism to control the topology for synchronization distribution. The Best Master Clock Algorithm (BMCA) defines the states for the PTP ports on a clock. One port will be set into slave state and the other ports will be set to master (or passive) states. Ports in slave state recovered synchronization delivered by from an external PTP clock and ports in master state transmit synchronization to toward external PTP clocks.

The basic synchronization timing computation between the PTP slave and PTP master is shown in Figure 18. This figure illustrates the offset of the slave clock referenced to the best master signal during startup.

Figure 18 PTP Slave and Master Time Synchronization Computation

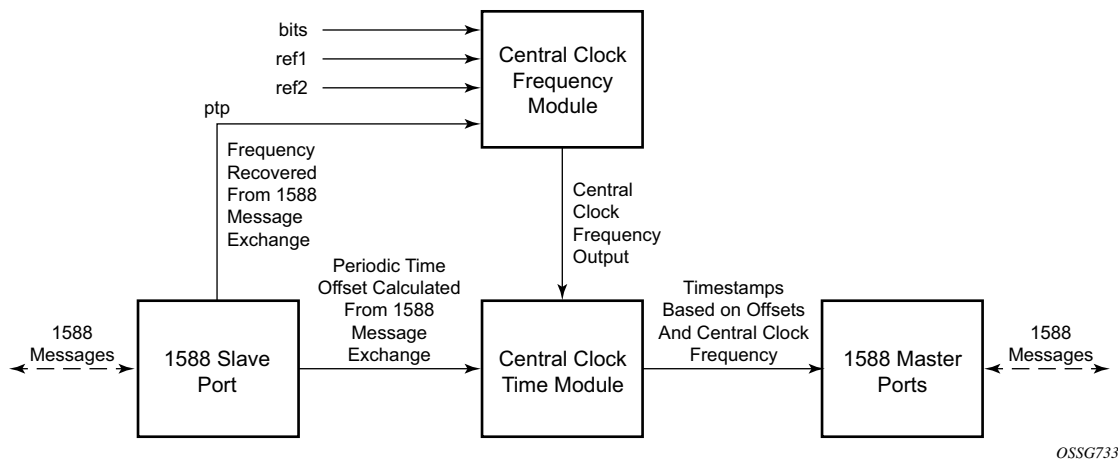


OSSG732

When using IEEE 1588v2 for distribution of a frequency reference, the slave calculates a message delay from the master to the slave based on the timestamps exchanged. A sequence of these calculated delays will contain information of the relative frequencies of the master clock and slave clock but will have noise component related to the packet delay variation (PDV) experienced across the network. The slave must filter the PDV effects so as to extract the relative frequency data and then adjust the slave frequency to align with the master frequency.

When using IEEE 1588v2 for distribution of time, the 7750 SR and 7450 ESS use the four timestamps exchanged using the IEEE 1588v2 messages to determine the offset between the router time base and the external master clock time base. The router determines the offset adjustment and then in between these adjustments, the router maintains the progression of time using the frequency from the central clock of the router. This allows time to be maintained using a BITS input source or a Synchronous Ethernet input source even if the IEEE 1588v2 communications fail. When using IEEE 1588v2 for time distribution, the central clock should at a minimum have a system timing input reference enabled.

Figure 19 Using IEEE 1588v2 For Time Distribution



5.5.6.2 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 grand master clock and the slave clock. In particular, when IEEE 1588v2 is used to distribute high accuracy time, such as for mobile base station phase requirements, then the network architecture requires the deployment of PTP awareness in every device between the Grandmaster and the mobile base station slave.

In addition, performance is also improved by the removal of any PDV caused by internal queuing within the boundary clock or slave clock. This is accomplished with hardware that is capable of detecting and time stamping the IEEE 1588v2 packets at the Ethernet interface. This capability is referred to as port-based time stamping.

5.5.6.2.1 Port-Based Timestamping of PTP Messages

For optimal performance, the 1588 packets should be time-stamped at the ingress and egress. This avoids any possible PDV that might be introduced between the port and the CPM. The ability to timestamp in the interface hardware is provided on a subset of the IMM and MDA assemblies of the routers. Refer to the release notes for the complete list.

In order for this to operate, the CPM, IOM, IMM, and MDAs must be running firmware that supports this capability. The CPM firmware upgrade occurs automatically when the CPM card software is updated. Since upgrading of IOM, IMM, and MDA firmware is service impacting, this upgrade is not performed automatically on a soft reset of the MDA. The IOM/IMM firmware is upgraded when the IOM/IMM card is hard reset. The MDA firmware is programmed during system initialization, when the MDA is inserted, or when the MDA is hard reset via a **clear mda** or **clear card** command. However, when an MDA is soft reset via either a **clear card soft** command or during a major ISSU, the MDA firmware is not updated.

5.5.6.3 PTP Capabilities

For each PTP message type to be exchanged between the router and an external 1588 clock, a Unicast Session must be established using the Unicast Negotiation procedures. The router allows configuration of the message rate to be requested from external 1588 clocks. The router also supports a range of message rates that it will grant to requests received from the external 1588 clocks.

[Table 37](#) describes the ranges for both the rates that the router can request and grant.

Table 37 Message Rates Ranges and Defaults

Message Type	Rates Requested by the 7450 ESS, 7750 SR, and 7950 XRS		Rates Granted by the 7450 ESS, 7750 SR, and 7950 XRS	
	Min	Max	Min	Max
Announce	1 packet every 16 seconds	8 packets/second	packet every 16 seconds	8 packets/second

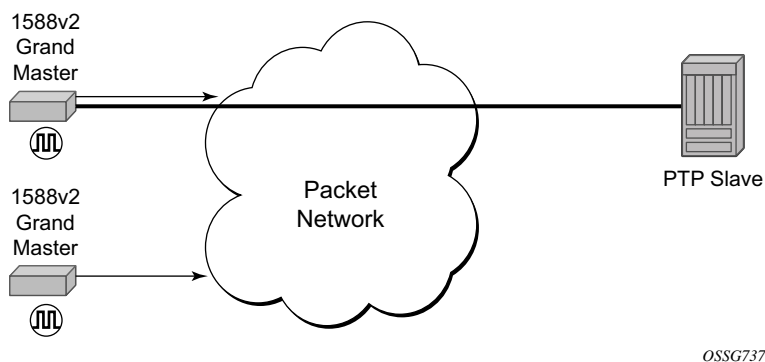
Table 37 Message Rates Ranges and Defaults (Continued)

Message Type	Rates Requested by the 7450 ESS, 7750 SR, and 7950 XRS		Rates Granted by the 7450 ESS, 7750 SR, and 7950 XRS	
	Min	Max	Min	Max
Sync	1 packet/second	64 packet/second	1 packet/second	128 packet/second
Delay_Resp	1 packet/second	64 packets/second	1 packet/second	128 packets/second
(Duration)	300	300	1	1000

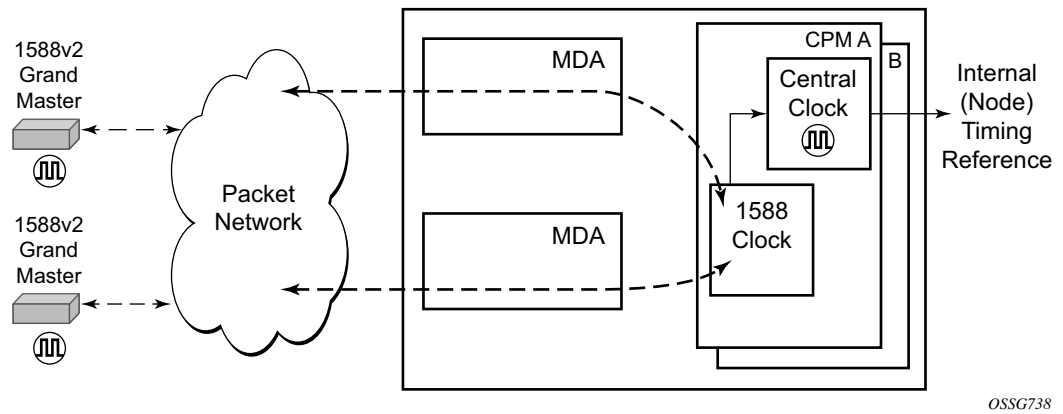
State and statistics data for each PTP peer are available to assist in the detection of failures or unusual situations.

5.5.6.4 PTP Ordinary Slave Clock For Frequency

Traditionally, only clock frequency is required to ensure smooth transmission in a synchronous network. The PTP ordinary clock with slave capability on the router provides another 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. [Figure 20](#) shows a PTP ordinary slave clock network configuration.

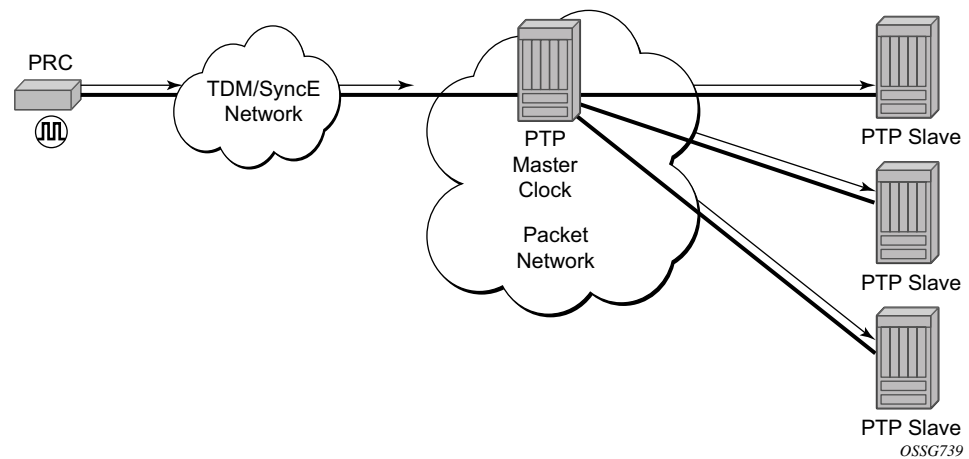
Figure 20 Slave Clock

The PTP slave capability is implemented on the CPM, version 3 or later. The IEEE 1588v2 messages can ingress and egress the router on any line interface. [Figure 21](#) shows the operation of an ordinary PTP clock in slave mode.

Figure 21 Ordinary Slave Clock Operation

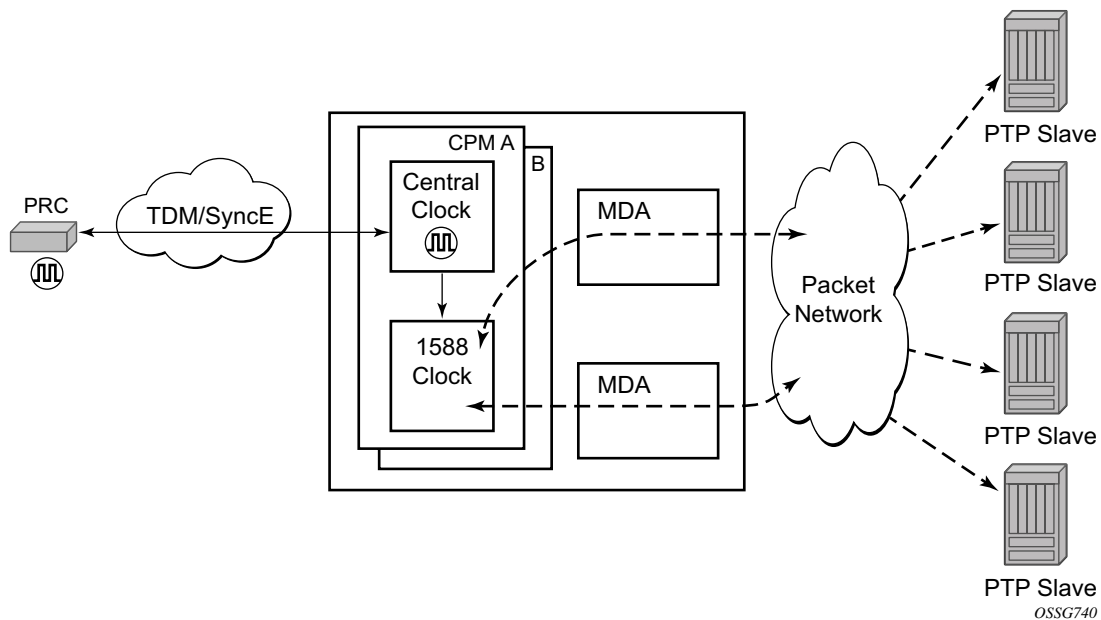
5.5.6.5 PTP Ordinary Master Clock For Frequency

The router supports the PTP ordinary clock in master mode. Normally, a IEEE 1588v2 grand master is used to support many slaves and boundary clocks in the network. In cases where only a small number of slaves and boundary clocks exist and only frequency is required, a PTP integrated master 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 master clock closer to the edge of the network, as close to the slave clocks as possible. [Figure 22](#) shows a PTP master clock network configuration.

Figure 22 PTP Master Clock

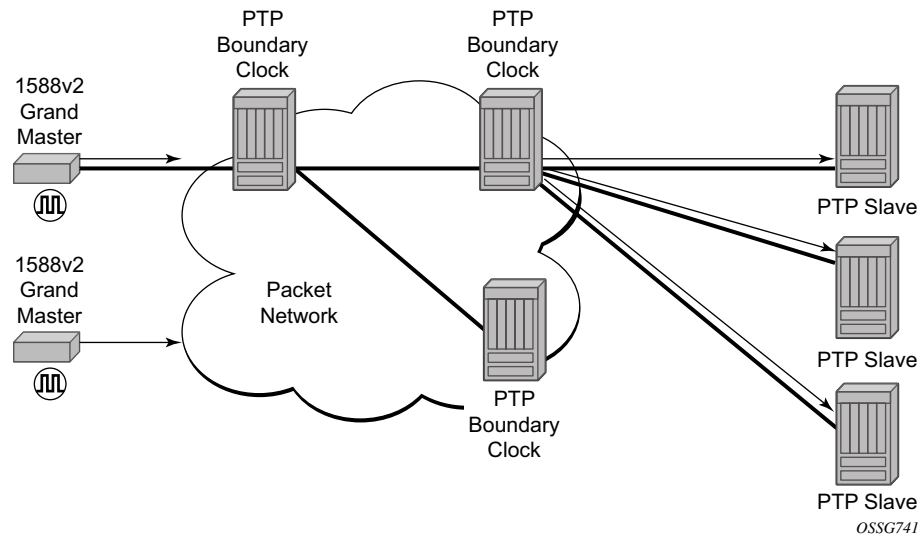
All packets are routed to their destination via the best route as determined in the route table; see [Figure 23](#). It does not matter which ports are used to ingress and egress these packets (unless port based time stamping is enabled for higher performance).

Figure 23 Ordinary Master Clock Operation



5.5.6.6 PTP Boundary Clock for Frequency and Time

The router supports boundary clock PTP devices in both master and slave 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, utilization rates, and the inherent behavior of the routers. By using routers with boundary clock functionality in the path between the grand master clock and the slave clock, one long path over many hops is split into multiple shorter segments, allowing better PDV control and improved slave performance. This allows PTP to function as a valid timing option in more network deployments and allows for better scalability and increased robustness in certain topologies, such as rings. Boundary clocks can simultaneously function as a PTP slave of an upstream grand master (ordinary clock) or boundary clock, and as a PTP master of downstream slaves (ordinary clock) and/or boundary clocks.

Figure 24 Boundary Clock

In addition, the use of port based timestamping in every network element between the grandmaster and the end slave application is highly recommended for delivering time to meet one microsecond accuracies required of mobile applications.

The router always uses the frequency output of the central clock to maintain the timebase within the router. The PTP reference into the central clock should always be enabled as an option if the router is configured as a boundary clock. This avoids the situation of the router entering holdover while propagating time with 1588.

5.5.6.7 PTP Clock Redundancy

The PTP module in the router exists on the CPM. The PTP module on the standby CPM is kept synchronized to the PTP module on the active CPM. All sessions with external PTP peers are maintained over a CPM switchover.

5.5.6.8 PTP Time for System Time and OAM Time

PTP has the potential to provide much more accurate time into the router than can be obtained with NTP. This PTP recovered time can be made available for system time and OAM packet time stamping to improve the accuracies of logged events and OAM delay measurements. The mechanism to activate PTP as the source for these internal time bases is to allocate PTP as a local server into NTP. This permits the

NTP time recovery to use PTP as a source for time and then distribute it within the router to system time and the OAM process. This activation also affects the operation of the NTP server within the SR OS. The PTP server appears as NTP stratum 0 server and therefore the SR OS will advertise itself as an NTP Stratum 1 server to external peers and clients. This activation may impact the NTP topology.

5.5.6.9 PTP within Routing Instances

In addition to Base routing and IES services, PTP messaging is supported within VPRN services on the 7750 SR and 7950 XRS platforms. The 7450 ESS supports PTP in the Base routing instance. PTP messaging is not supported through the management router instance. Only one PTP clock exists within the router and it is shared by all routing instances that have access. Only one routing instance may have configured peers and only this routing context can receive the time or frequency reference into the router (contain a PTP port in Slave state). The dynamic peers are shared across all routing instances; if it is desired to control the number of dynamic peers that can be consumed by a given routing instance then this must be configured for that routing instance.

5.6 System-Wide ATM Parameters

On the 7750 SR, the atm-ping OAM loopback feature for can be enabled on an ATM SAP for a period of time configured through the interval and the send-count parameters. When the ATM SAP terminates on IES or VPRN services, a failure of the loopback state machine does not bring down the Layer 3 interface. Only receiving AIS/RDI OAM cells or entering the AIS/RDI state brings down the Layer 3 interface.

The atm-ping OAM loopback feature can be also be enabled on a continuous basis on an ATM SAP terminating on IES or VPRN services. When the loopback state machine fails, the Layer 3 interface is brought down.

The ATM OAM loopback parameters must be first enabled and configured in the **config>system> atm>oam** context and then enabled in the IES or VPRN service interface SAP **atm oam** context.

Refer to the IES and VPRN sections of the *Layer 3 Services Guide* for further information.

5.7 Link Layer Discovery Protocol (LLDP)

The IEEE 802.1ab Link Layer Discovery Protocol (LLDP) is a unidirectional protocol that uses the MAC layer to transmit specific information related to the capabilities and status of the local device. Separately from the transmit direction, the LLDP agent can also receive the same kind of information for a remote device which is stored in the related MIBs.

LLDP itself does not contain a mechanism for soliciting specific information from other LLDP agents, nor does it provide a specific means of confirming the receipt of information. LLDP allows the transmitter and the receiver to be separately enabled, making it possible to configure an implementation so the local LLDP agent can either transmit only or receive only, or can transmit and receive LLDP information.

The information fields in each LLDP frame are contained in a LLDP Data Unit (LLDPDU) as a sequence of variable length information elements, that each include type, length, and value fields (known as TLVs), where:

- Type identifies what kind of information is being sent.
- Length indicates the length of the information string in octets.
- Value is the actual information that needs to be sent (for example, a binary bit map or an alphanumeric string that can contain one or more fields).

Each LLDPDU contains four mandatory TLVs and can contain optional TLVs as selected by network management:

- Chassis ID TLV
- Port ID TLV
- Time To Live TLV
- Zero or more optional TLVs, as allowed by the maximum size of the LLDPDU
- End Of LLDPDU TLV

The chassis ID and the port ID values are concatenated to form a logical identifier that is used by the recipient to identify the sending LLDP agent/port. Both the chassis ID and port ID values can be defined in a number of convenient forms. Once selected however, the chassis ID/port ID value combination remains the same as long as the particular port remains operable.

A non-zero value in the TTL field of the time-to-live TLV tells the receiving LLDP agent how long all information pertaining to this LLDPDU's identifier will be valid so that all the associated information can later be automatically discarded by the receiving LLDP agent if the sender fails to update it in a timely manner. A zero value indicates that any information pertaining to this LLDPDU's identifier is to be discarded immediately.

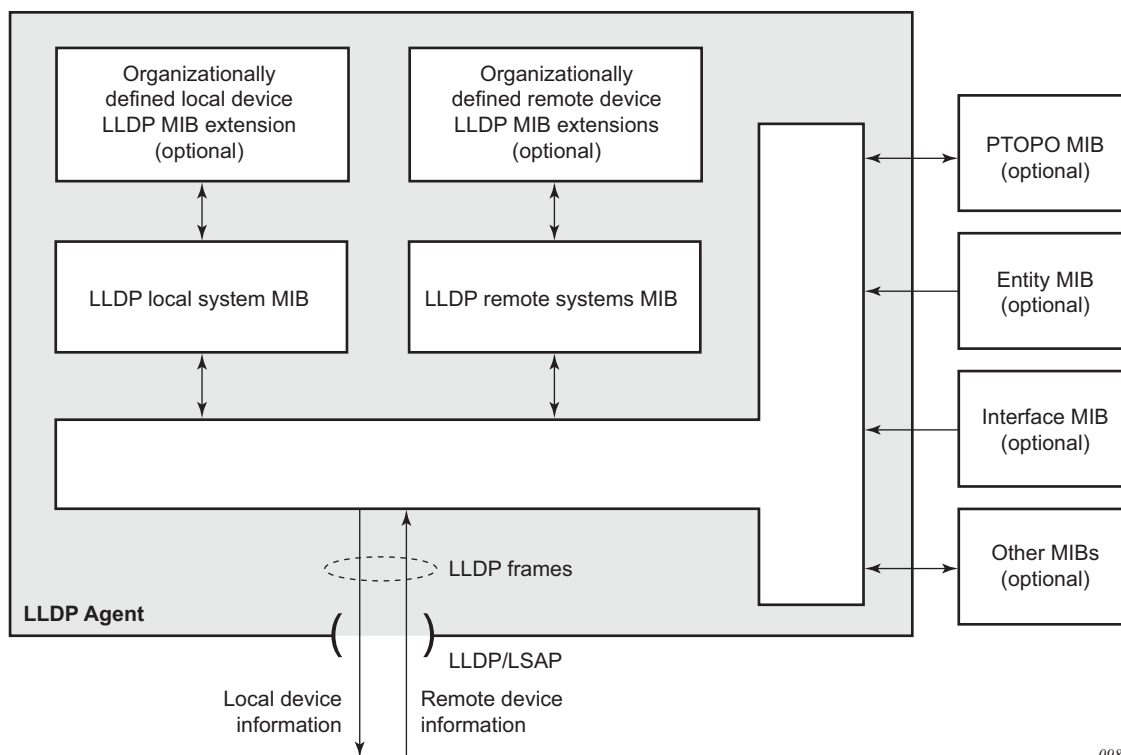
A TTL value of zero can be used, for example, to signal that the sending port has initiated a port shutdown procedure.

The end of a LLDPDU TLV marks the end of the LLDPDU.

The IEEE 802.1ab standard defines a protocol that:

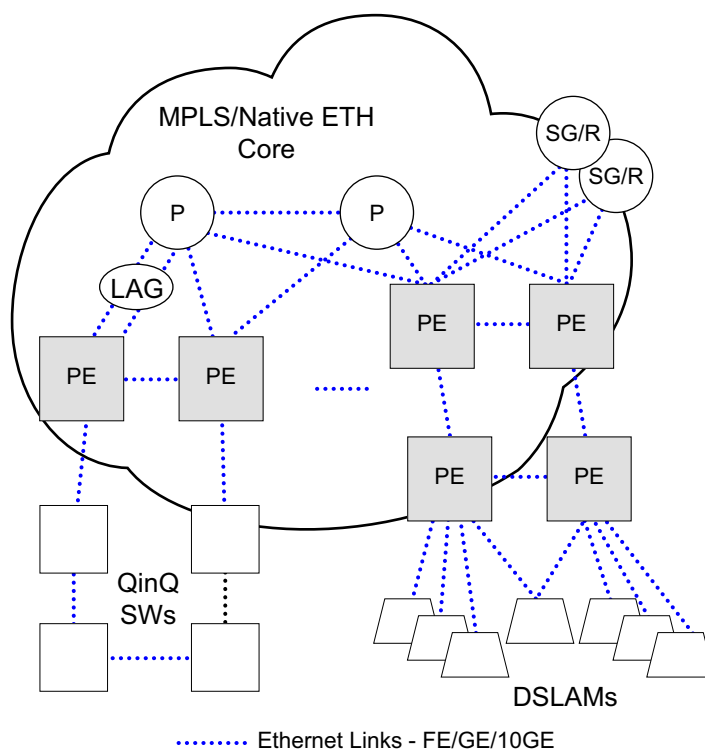
- Advertises connectivity and management information about the local station to adjacent stations on the same IEEE 802 LAN.
- Receives network management information from adjacent stations on the same IEEE 802 LAN.
- Operates with all IEEE 802 access protocols and network media.
- Establishes a network management information schema and object definitions that are suitable for storing connection information about adjacent stations.
- Provides compatibility with a number of MIBs as depicted in [Figure 25](#).

Figure 25 LLDP Internal Architecture for a Network Node



0981

Network operators must be able to discover the topology information in order to detect and address network problems and inconsistencies in the configuration. Moreover, standard-based tools can address the complex network scenarios where multiple devices from different vendors are interconnected using Ethernet interfaces.

Figure 26 Customer Use Example For LLDP

OSSG263

The example displayed in [Figure 26](#) depicts a MPLS network that uses Ethernet interfaces in the core or as an access/hand off interfaces to connect to different kind of Ethernet enabled devices such as service gateway/routers, QinQ switches, DSLAMs or customer equipment.

IEEE 802.1ab LLDP running on each Ethernet interfaces in between all the above network elements may be used to discover the topology information.

5.8 IP Hashing as an LSR

It is now possible to include IP header in the hash routine at an LSR for the purpose of spraying labeled-IPv4 and labeled-IPv6 packets over multiple equal cost paths in ECMP in an LDP LSP and/or over multiple links of a LAG group in all types of LSPs.

A couple of configurable options are supported. The first option is referred to as the Label-IP Hash option and is designated in the CLI as **lbl-ip**. When enabled, the hash algorithm parses down the label stack and once it hits the bottom of the stack, it checks the next nibble. If the nibble value is four or six then it will assume it is an IPv4 or IPv6 packet. The result of the hash of the label stack, along with the incoming port and system IP address, is fed into another hash along with source and destination address fields in the IP packet's header. The second option is referred to as IP-only hash and is enabled in CLI by entering the **iponly** keyword. It operates the same way as the Label-IP Hash method except the hash is performed exclusively on the source and destination address fields in the IP packet header. This method supports both IPv4 and IPv6 payload and operates on packets received on an IP interface on an IOM3-XP/IMM port only.

By default, MPLS packet hashing at an LSR is based on the whole label stack, along with the incoming port and system IP address. This method is referred to as Label-Only Hash option and is enabled in CLI by entering the **lbl-only** keyword.

The **lbl-only**, **lbl-ip** and **ip-only** hashing options can be configured system-wide and can also be overridden on a per-IP-interface basis.

The **ip-only** option and the IPv6 payload support with the **lbl-ip** option can only be enabled on IP interfaces on IOM3/IMM ports.

5.9 Ethernet Satellites

The Ethernet satellite support feature allows a 7210 SAS-S chassis to act as a port extension for the 7750 SR host. In this configuration, all configuration and management functions are performed through the host node. Management of the SAS-S node is not required when it is configured in an Ethernet satellite operations mode.

[Table 38](#) lists the supported Ethernet satellite chassis.

Table 38 **Supported Ethernet Satellite Chassis**

Chassis Type	Sat-Type String
24-port fiber	es24-1gb-sfp
48-port fiber	es48-1gb-sfp

The following primary tasks must be performed to configure an Ethernet satellite.

1. Create a software repository that specifies where the 7210 SAS-S should obtain its correct software image.
2. Create an Ethernet satellite association that binds an Ethernet chassis to a set of uplinks and a software repository.
3. Configure the satellite ports to specify port configuration and service association.

5.9.1 Software Repositories for Satellites

The software repositories define the locations from where the host can obtain software for subcomponents including Ethernet satellites. The software repository is also used to upgrade an existing subcomponent by changing the location of the image to be served to the remote device. The software repositories are not used for management of the host router software, which is managed using the standard procedures described in the Release Notes.

Each software repository supports up to three locations to search for the software. A location may be a URL or a directory on a compact flash. When an upgrade operation is initiated, each of the three locations is checked in sequence to locate the required software. The upgrade operation will fail if the software is not located in any of the configured locations. The satellite booting operation will also fail if the software cannot be located.

At least one software repository must be configured to support a satellite connected to the local host by using the **config>system>software-repository** CLI tree as follows.

- Create a software repository using a unique repository name.
- Specify the primary location for the 7210 SAS-S image.
- Optionally, specify a secondary or tertiary image location and a description.

5.9.2 Satellite Software Upgrade Overview

The process to change or upgrade the satellite software consists of the following steps.

1. Copy the new satellite software images to a local compact flash card. It is recommended that the new image files be placed in a different directory.
Although you can store the satellite software on a remote server and use a URL to reference the remote location, it is recommended that the primary image location is locally accessible.
2. Create a new software repository using a new name and at least a primary-location for the 7210 SAS-S image.
3. Modify the 7210 SAS-S satellite configuration such that the **software-repository** parameter references the newly created software repository.

Use the following CLI context:

config>system>satellite>esat-sat sat-id

4. Reboot the Ethernet satellite to load the new software.

Depending on whether a firmware update is needed, perform one of the following steps to reboot the 7210 SAS-Sx.

- a. 7210 SAS-Sx firmware update not required

- i. The Ethernet satellite loads the new software the next it reboots.
- ii. You can reset the Ethernet satellite with the following administrative command, if required.

admin satellite eth-sat <sat-id> reboot [now]

- b. 7210 SAS-Sx firmware update required

- i. To continue the upgrade to the 7210 firmware image, enter the following command and allow it to complete:

admin satellite eth-sat x sync-boot-env

- ii. Reboot the satellite again using the **upgrade** keyword to update the firmware image.

The **upgrade** keyword causes the 7210 SAS-S to upgrade the included firmware images. This process takes longer than a normal reboot.

admin satellite eth-sat x reboot upgrade now

5.9.3 Satellite Configuration

After creating the software repositories, the next step is to configure the Ethernet satellite. The satellite configuration is required to create a satellite binding to a satellite ID, and to provide additional information that will uniquely identify the satellite chassis, chassis type, and the software repository to be used to boot the remote Ethernet satellite.

The following parameters must be specified for an Ethernet satellite.

- **mac-address** - The Ethernet satellite chassis MAC address must be specified. This is used to bind a specific Ethernet chassis to the associated satellite ID. (The local host router will boot only satellites with configured MAC addresses.)
- **sat-type** - The satellite chassis type must be specified and must match the chassis type that the satellite advertises during the boot process.
- **software-repository** - A preconfigured software repository must be specified in the satellite configuration. This defines the location of the software image to boot the associated 7210 SAS-S.
- **no shutdown** - By default, a new satellite is in a shutdown state; use the **no shutdown** command to bring the satellite online.

The following parameters are optional for an Ethernet satellite.

- **description** - Use this command to configure a description string associated with the satellite.
- **sync-e** - Use this command to enable the **sync-e** option.

5.9.3.1 Satellite Client Port Association

Use the following format to reference Ethernet satellite client ports:

port esat- *sat-id/1/sat-port*

5.10 Optical Extension Shelf (OES)

The OES is an add-on chassis for the 7750 SR and 7950 XRS routers that provides the capability to originate Dense Wavelength Division Multiplexing (DWDM) interfaces from the node. The OES is fully managed through the 7750 SR and 7950 XRS routers and is an integral part of the routing architecture. Configuration and monitoring of OES elements is performed through the router.

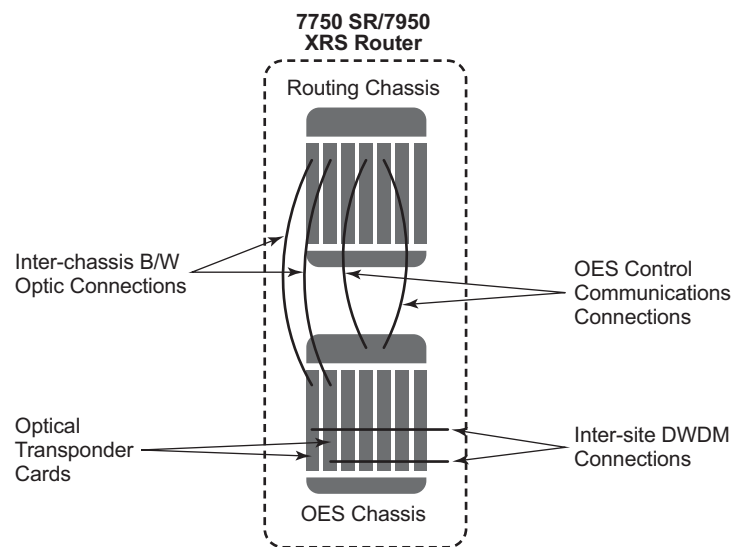


Note: OES is only supported on the 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7950 XRS-20, and 7950 XRS-40 routers.

A 10 G or 100 G router interface can be connected into a muxponder within the OES, providing translation between black and white optics and colored optics used for DWDM transport. This allows for longer reach and bandwidth efficiency of inter-site optical fiber. OES hardware assemblies are based on 1830 PSS assemblies from Nokia's IP/Optical Networking group.

As shown in [Figure 27](#), there are redundant control communication links between the router chassis and the OES chassis. These allow the router to control the elements within the OES chassis. Black and white (B/W) ports on the router can be connected to B/W ports on the muxponder cards within the OES chassis. The colored line port of a muxponder card can then be programmed for the specific DWDM frequency that will be generated. These DWDM signals can then be multiplexed and carried over DWDM networks using external filters and amplifiers.

Figure 27 OES Platform



1019

To use the OES, the OES chassis must be installed and control communications established as described in the *7750 SR and 7950 XRS Optical Extension Shelf Installation Guide*.

When installed, the OES chassis appears as a new chassis within the router configuration. The chassis is identified using the chassis number, for example, oes-1.

Cards are identified by their slot numbers within the chassis, for example, oes-1/8.

Ports are identified by the identifier on the card, for example, oes-1/8/c1 or oes-1/8/l1 identifies the first client port and first line port on the muxponder in slot 8 of the OES chassis.

It is recommended to add the router port to the OES client port connections in the router's port topology. This facilitates correlation of events on the router to events on the OES.

The following optical muxponders are supported in the OES chassis.

Table 39 **Optical Muxponders Supported in OES Chassis**

Optical Muxponder	Description
260SCX2	Either 1 or 2 ports 100 GE to one DWDM wavelength
130SCX10	Up to 10 ports 10 GE to one DWDM wavelength

The 260SCX2 card can operate in 130 G mode (one 100 GE port) or 260 G mode (two 100 GE ports). Up to eight of the 260SCX2 cards can be used if they all operate in 130 G mode, and seven if any of the cards operate in 260 G mode.

5.11 Administrative Tasks

This section contains information to perform administrative tasks.

- [Configuring the Chassis Mode](#)
- [Saving Configurations](#)
- [Specifying Post-Boot Configuration Files](#)
- [Network Timing](#)
- [Power Supplies](#)

5.11.1 Configuring the Chassis Mode

Depending on the 7450 ESS and 7750 SR chassis type and IOM type, the following modes can be configured:



Note: Chassis modes are not available on the 7750 SR-c12 router.

- a:** This mode corresponds to scaling and feature set associated with iom-20g.
- b:** This mode corresponds to scaling and feature set associated with iom-20g-b.
- c:** This mode corresponds to scaling and feature set associated with iom2-20g.
- d:** This mode corresponds to scaling and feature set associated with iom3-xp.

If the chassis mode is not explicitly provisioned in the configuration file, the chassis will come up in chassis mode a by default. The behavior for the IOMs is described in the following table:

Table 40 **Provisioned IOM Card Behavior**

IOM	Behavior
iom-20g-b	Comes online if provisioned as iom-20g or iom-20g-b.
iom2-20g	Comes online if provisioned as iom-20g, iom-20g-b or iom2-20g.
iom-10g	Comes online if provisioned as iom-10g (7450 ESS only).
iom3-xp	Comes online if provisioned as iom3-xp.

To support a particular chassis-mode, all provisioned IOMs must meet the corresponding IOM level.

The chassis Mode corresponds to scaling and feature sets associated with a given card. The base mode is chassis mode A which supports all IOM card types.

IOM cards that are not compatible with more recent 7750 SR chassis modes will be put into an operationally failed state if the configuration chassis mode **force** option is used.

- Chassis mode A corresponds to iom-20g, chassis mode backwards compatible for iom-20g-b, iom2-20g, iom3-xp
- Chassis mode B corresponds to iom-20g-b, chassis mode backwards compatible for iom2-20g, iom3-xp
- Chassis mode C corresponds to iom2-20g, chassis mode backwards compatible for iom3-xp
- Chassis mode D corresponds to iom3-xp

IOM cards that are not compatible with more recent 7450 ESS chassis modes will stay or be put into an operationally down state.

- Chassis mode A corresponds to iom-20g, chassis mode backwards compatible for iom-20g-b, iom2-20g, iom3-xp
- Chassis mode B corresponds to iom-20g-b, chassis mode backwards compatible for iom2-20g, iom3-xp
- Chassis mode D corresponds to iom3-xp



Note: The iom-20g is not supported from 5.0R and later but chassis mode A is described for backwards compatibility purposes.

The **force** keyword forces an upgrade either from mode **a** to mode **b** or **d** with cards provisioned as iom-20g or from mode **b** to mode **c** with cards provisioned as iom-20g-b (7750 SR).

On the 7750 SR, the ASAP MDA can only be configured if the IOM2-20g and IOM3-XP is provisioned.

If you are in chassis-mode **d** and configure an IOM type as iom2-20g and then downgrade to chassis-mode **a** or **b** (you must specify **force** keyword), a warning appears about the IOM downgrade. In this case, the IOM's provisioned type will downgrade to iom-20g-b. Once this is done, the ASAP MDA cannot be configured. The following message appears:

```
*A:138.120.214.68>config>system# chassis-mode b
MINOR: CHMGR #1009 Mode change requires force - card-type iom2-20g in slot 1 would
change to iom-20g-b *A:138.120.214.68>config>system# chassis-mode b force
MINOR: CHMGR #1010 Can not change mode - mda m1-choc12-as-sfp in 10/1 not supported
when card changes to iom-20g-b
```

If this is the desired behavior, for example, chassis-mode **d** is configured and IPv6 is running, you can then downgrade to chassis-mode **a** or **b** if you want to disable IPv6.

```
*A:ALA-48# show chassis
=====
Chassis Information
=====
Name                : ALA-48
Type                : 7750 SR-12
Location            : exit
Coordinates          : N 45 58 23, W 34 56 12
CLLI code           : abcdefg1234
Number of slots      : 12
Number of ports      : 246
Critical LED state   : Off
Major LED state      : Off
Minor LED state      : Off
```

```

Over Temperature state          : OK
Base MAC address                : 14:30:ff:00:00:00
Admin chassis mode              : d
Oper chassis mode                : d

Hardware Data
  Part number                    : Sim Part#
  CLEI code                      : Sim CLEI
  Serial number                  : sim48
  Manufacture date               : 01012003
  Manufacturing string            : Sim MfgString sim48
  Manufacturing deviations        : Sim MfgDeviation sim48
  Time of last boot              : 2007/09/24 08:15:17
  Current alarm state            : alarm cleared
-----
Environment Information
...
=====
*A:ALA-48#

```

5.11.2 Saving Configurations

Whenever configuration changes are made, the modified configuration must be saved so they will not be lost when the system is rebooted.

Configuration files are saved by executing explicit command syntax which includes the file URL location to save the configuration file as well as options to save both default and non-default configuration parameters. Boot option 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 boot option files, refer to [Boot Options](#).

5.11.3 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 certain commands enabled or disabled, or particular parameters specified and according to the script which loads that file.

5.11.4 Network Timing

In Time Domain Multiplexed (TDM)-based networks (for example, SONET or SDH circuit-switched networks), the concept of network timing is used to prevent over-run or under-run issues where circuits are groomed (rebundled) and switched. Hardware exists in each node that takes a common clock derived from an internal oscillator, a specific receive interface, or special BITS interface and provides it to each synchronous interface in the system. Usually, each synchronous interface is allowed to choose between using the chassis-provided clock or the clocking recovered from the received signal on the interface. The clocking is used to drive the transmit side of the interface. The appropriate configuration at each node which defines how interface clocking is handled must be considered when designing a network that has a centralized timing source so each interface is operating in a synchronous manner.

The effect of timing on a network is dependent on the nature of the type of traffic carried on the network. With bit-wise synchronous traffic (traditional circuit-based voice or video), non-synchronous transmissions cause a loss of information in the streams affecting performance. With packet-based traffic, the applications expect and handle jitter and latency inherent to packet-based networks. When a packet-based network is used to carry voice or video traffic, the applications use data compression and elasticity buffering to compensate for jitter and latency. The network itself relies on appropriate Quality of Service (QoS) definitions and network provisioning to further minimize the jitter and latency the application may experience.

5.11.5 Power Supplies

SR OS supports a **power-supply** command to configure the type and number of power supplies present in the chassis. The operational status of a power source is always displayed by the LEDs on the Control Processor/Switch Fabric Module (CP/SFM) front panel, but the power supply information must be explicitly configured in order for a power supply alarm to be generated if a power source becomes operationally disabled.

5.11.6 Automatic Synchronization

Use the CLI syntax displayed below to configure synchronization components relating to active-to-standby CPM switchover. In redundant systems, synchronization ensures that the active and standby CPMs have identical operational parameters, including the active configuration, CPM, XCM, and IOM images in the event of a failure or reset of the active CPM.

The **force-switchover** command forces a switchover to the standby CPM 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.cfg, primary/secondary/tertiary configuration files (.cfg and .ndx), li, and ssh 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 and when an **admin>save** command is entered with no filename specified.

5.11.6.1 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 CPM (in redundant systems). The synchronization parameters on the standby CPM are preserved.
2. The primary, secondary, and tertiary images, (provided they are locally stored on the active CPM) are copied to the same compact flash on the standby CPM.
3. The primary, secondary, and tertiary configuration files, (provided they are locally stored on the active CPM) are copied to the same compact flash on the standby CPM.

5.11.6.2 Config Option

The **config** option synchronizes configuration files by copying the files specified in the active CPM BOF file to the same compact flash on the standby CPM.

Both image files (CPM and IOM) on the 7450 ESS must be located in the same directory. Failure to locate and synchronize both images causes an error to be generated.

5.11.7 Manual Synchronization

The **admin redundancy synchronize** command performs manual CPM 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.

5.11.7.1 Forcing a Switchover

The **force-switchover now** command forces an immediate switchover to the standby CPM card.

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

5.12 System Router Instances

SR OS supports multiple Layer 3 router instances. These instances have their own IP addressing spaces and parameters. Router instances are isolated from each other.

The following are the different types of router instances in SR OS:

- **Base**

All SR OS routers have the Base router instance: the system created default router instance used to forward user IP traffic among router line card ports. Router interfaces (that is, network interfaces configured under **configure router [Base]**) and IES services and interfaces exist in the Base router instance. The Base router instance is identified in SNMP as vRtrType = baseRouter (1) and has a vRtrID of 1.

- **VPRN instances**

Another type of router instance is the set of operator configured VPRN services. Each VPRN service has a unique router instance. For more information about VPRN services and their associated router instances, see the SR OS Layer 3 Services Guide. VPRN router instances are identified in SNMP as vRtrType = vprn (2), and the vRtrID is dynamically allocated.

- **Special system router instances**

SR OS routers also support the following special router instances:

- **management**

The management router instance is a system created router instance that is used for management of the router. The management router instance is bound to CPM/CFM/CCM ports A/1 and B/1. This is a CPM router instance which cannot be renamed or deleted by an operator. The management router instance is identified in SNMP as vRtrType = vr(3), and the vRtrID is 4095.

- **vpls-management**

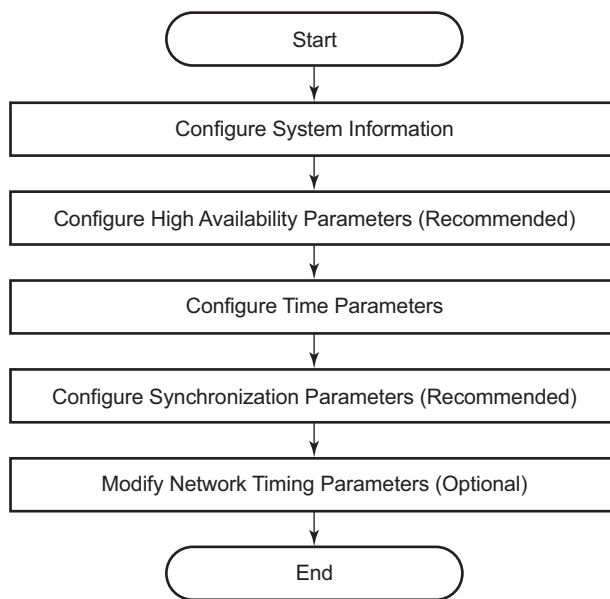
The vpls-management router instance is used for management of VPLS services. It is identified in SNMP as vRtrType = vr(3), and the vRtrID is 4094.

- **User created CPM router instances**

User created CPM router instances are user defined router instances that are mainly used with ethernet ports on the CPM/CFM/CCM cards: CPM router instances only use CPM/CFM/CCM ethernet ports as interfaces. CPM router instances have a user-defined name and are the only types of non-VRPN router instances that can be created by the user. User created CPM router instances are identified in SNMP as vRtrType = vr(3), and the vRtrID is dynamically allocated.

5.13 System Configuration Process Overview

Figure 28 shows the process to provision basic system parameters.

Figure 28 System Configuration and Implementation Flow

7750_SR_Basics_27

5.14 Configuration Notes

This section describes system configuration caveats.

5.14.1 General

The system must be properly initialized and the boot loader and BOF files successfully executed in order to access the CLI.

5.15 Configuring System Management with CLI

This section provides information about configuring system management features with CLI.

Topics in this chapter include:

- [Basic System Configuration](#)
- [Common Configuration Tasks](#)
- [System Information](#)
 - [System Information Parameters](#)
 - [Name](#)
 - [Contact](#)
 - [Location](#)
 - [CLLI Code](#)
 - [Coordinates](#)
 - [System Time Elements](#)
 - [Zone](#)
 - [Summer Time Conditions](#)
 - [NTP](#)
 - [SNTP](#)
 - [CRON](#)
 - [Configuring Synchronization and Redundancy](#)
 - [Configuring Synchronization](#)
 - [Configuring Manual Synchronization](#)
 - [Forcing a Switchover](#)
 - [Configuring Synchronization Options](#)
 - [Configuring Multi-Chassis Redundancy for LAG](#)
- [Configuring Mixed Mode](#)
- [Configuring Power Supply Parameters](#)
- [Post-Boot Configuration Extension Files](#)
- [System Timing](#)
 - [Edit Mode](#)
 - [Configuring Timing References](#)
 - [Using the Revert Command](#)
 - [Other Editing Commands](#)

- [Forcing a Specific Reference](#)
- [Configuring System Monitoring Thresholds](#)
- [Configuring LLDP](#)

5.16 System Management

5.16.1 Saving Configurations

Whenever configuration changes are made, the modified configuration must be saved so the changes will not be 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 option file (BOF) parameters. For more information about boot option files, refer to the [Boot Options](#).

Configuration files are saved by executing *implicit* or *explicit* 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, path IDs, etc. 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.

5.17 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 shows a basic system configuration:

```
A:ALA-12>config>system# info
#-----
echo "System Configuration "
#-----
      name "ALA-12"
      coordinates "Unknown"
      snmp
      exit
      security
        snmp
          community "private" rwa version both
        exit
      exit
      time
        ntp
          server 192.168.15.221
          no shutdown
        exit
        snmp
          shutdown
        exit
        zone GMT
      exit
#-----
A:ALA-12>config>system#
```

5.18 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](#)
 - [Name](#)
 - [Contact](#)
 - [Location](#)

- [CLLI Code](#)
 - [Coordinates](#)
- [System Time Elements](#)
 - [Zone](#)
 - [Summer Time Conditions](#)
 - [NTP](#)
 - [SNTP](#)
 - [CRON](#)
 - [Schedule](#)
- [Synchronization and Redundancy](#)
 - [Automatic Synchronization](#)
 - [Manual Synchronization](#)
- [System Timing](#)
 - [Configuring Timing References](#)

5.18.1 System Information

This section covers the basic system information parameters to configure the physical location of the router, contact information, location information such as the place the router is located such as an address, floor, room number, etc., global positioning system (GPS) coordinates, and system name.

Use the CLI syntax shown below to configure the following system components:

- [System Information Parameters](#)
- [System Time Elements](#)

General system parameters include:

- [Name](#)
- [Contact](#)
- [Location](#)
- [CLLI Code](#)
- [Coordinates](#)

5.18.1.1 System Information Parameters

5.18.1.1.1 Name

Use the **system** 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 ALA-12`

The following example shows the system name:

```
sysName@domain>config>system# info
#-----
echo "System Configuration "
#-----
      name "ALA-12"
. . .
      exit
-----
sysName@domain>config>system#
```

5.18.1.1.2 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"`

5.18.1.1.3 Location

Use the **location** command to specify the system location of the device. For example, enter the city, building address, floor, room number, etc., 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"`

5.18.1.1.4 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 an SR-series router.

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`

5.18.1.2 Coordinates

Use the optional **coordinates** command to specify the GPS location of the device. If the string contains special characters (#, \$, spaces, etc.), 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 shows the configuration output of the general system commands:

```
sysName@domain>config>system# info
#-----
echo "System Configuration "
#-----
name "ALA-12"
    contact "Fred Information Technology"
    location "Bldg.1-floor 2-Room 201"
    clli-code "abcdefg1234"
    coordinates "N 45 58 23, W 34 56 12"
. . .
```

```
exit
```

```
A:ALA-12>config>system#
```

5.18.1.3 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 show time according to the local time zone.

Time elements include:

- Zone
- Summer Time Conditions
- NTP
- SNTP

5.18.1.3.1 Zone

The **zone** command sets the time zone and/or time zone offset for the router. The router supports system-defined and user-defined time zones. The system-defined time zones are listed in [Table 41](#).

CLI Syntax: `config>system>time`

zone	std-zone-name	non-std-zone-name
	[hh [:mm]]	

```
Example: config>system>time#  
config>system>time# zone GMT
```

The following example shows the zone output:

```
A:ALA-12>config>system>time# info
-----
ntp
                                server 192.168.15.221
                                no shutdown
exit
sntp
                                shutdown
exit
zone UTC
-----
A:ALA-12>config>system>time#
```

Table 41 **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
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 (e.g., Perth)	UTC +8 hours

Table 41 System-defined Time Zones (Continued)

Acronym	Time Zone Name	UTC Offset
ACST	Central Standard Time (e.g., Darwin)	UTC +9.5 hours
AEST	Eastern Standard/Summer Time (e.g., Canberra)	UTC +10 hours
NZT	New Zealand Standard Time	UTC +12 hours
NZDT	New Zealand Daylight Saving Time	UTC +13 hours

5.18.1.3.2 Summer Time Conditions

The **config>system>time>dst-zone** context 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 will be 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
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 41](#), 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 will return an error if the start and ending dates and times are not available either in [Table 41](#) or entered as optional parameters in this command.

The following example shows the configured parameters.

```
A:ALA-48>config>system>time>dst-zone# info
```

```
start second sunday april 02:00
end first sunday october 02:00
offset 0
-----
A:ALA-48>config>system>time>dst-zone# offset 0
```

5.18.1.3.3 NTP

Network Time Protocol (NTP) is 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 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](#)
- [Broadcast](#)
- [Broadcastclient](#)
- [Multicast](#)
- [Multicastclient](#)
- [NTP-Server](#)
- [Peer](#)
- [Server](#)

Authentication-check

NTP supports an authentication mechanism to provide some security and access control to servers and clients. The default behavior when any authentication keys are configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type, or key. The authentication-check command provides for the options to skip or maintain this rejection of NTP PDUs that do not match the authentication requirements.

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#
config>system>time>ntp# authentication-check
config>system>time>ntp# no shutdown
```

Authentication-key

The **authentication-key** 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#
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:sim1>config>system>time>ntp# info
-----
shutdown
authentication-key 1 key "OAwgNULbzgI" hash2 type des
-----
A:sim1>config>system>time>ntp#
```

Broadcast

The **broadcast** command is used to transmit broadcast packets on a given interface. Interfaces in the base routing context or the management interface may be specified. Due the relative ease of spoofing of broadcast messages, it is strongly recommended to use authentication with broadcast mode. The messages are transmitted using a destination address that is the NTP Broadcast address.

CLI Syntax:

```
config>system>time>ntp
    broadcast [router router-name] {interface
    ip-int-name} [key-id key-id] [version
    version]
    [ttl ttl]
```

Example:

```
config>system>time>ntp#
config>system>time>ntp# broadcast interface int11
version 4
ttl 127
config>system>time>ntp# no shutdown
```

The following example in the **system>time** context shows NTP enabled with the broadcast command configured.

```
A:sim1>config>system>time# info detail
-----
ntp
no shutdown
authentication-check
ntp-server
broadcast interface int11 version 4 ttl 127
exit
A:sim1>config>system>time#
```

5.18.1.3.4 Broadcastclient

The **broadcastclient** command enables listening to NTP broadcast messages on the specified interface. Interfaces in the base routing context or the management interface may be specified. Due the relative ease of spoofing of broadcast messages, it is strongly recommended to use authentication with broadcast mode. The messages must have a destination address of the NTP Broadcast address.

CLI Syntax:

```
config>system>time>ntp
                        broadcastclient [router router-name]
                        {interface ip-int-name}
                        [authenticate]
```

Example:

```
config>system>time>ntp#
config>system>time>ntp# broadcastclient interface int11
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the broadcastclient parameter enabled.

```
A:ALA-12>config>system>time# info
-----
ntp
broadcastclient interface int11
no shutdown
exit
-----
A:ALA-12>config>system>time#
```

Multicast

When configuring NTP the node can be configured to transmit or receive multicast packets on the CPM MGMT port (CPM applies to the 7450 ESS and 7750 SR). Broadcast & Multicast messages can easily be spoofed, therefore, authentication is strongly recommended. Multicast is used to configure the transmission of NTP multicast messages. The **no** construct of this command removes the transmission of multicast packets on the management port.

When transmitting multicast NTP messages the default address of 224.0.1.1 is used.

CLI Syntax: `config>system>time>ntp`
 `multicast [version version] [key-id key-id]`

Example: `config>system>time>ntp#`
 `config>system>time>ntp# multicast`
 `config>system>time>ntp# no shutdown`

The following example shows NTP enabled with the multicast command configured.

```
A:ALA-12>config>system>time# info
-----
server 192.168.15.221
multicast
no shutdown
-----
A:ALA-12>config>system>time#
```

Multicastclient

The **multicastclient** command is used to configure an address to receive multicast NTP messages on the CPM MGMT port (7450 ESS and 7750 SR). Broadcast & Multicast messages can easily be spoofed, therefore, authentication is strongly recommended. The **no** construct of this command removes the multicast client. If multicastclient is not configured, all NTP multicast traffic will be ignored.

CLI Syntax: `config>system>time>ntp`
 `multicastclient [authenticate]`

Example: `config>system>time>ntp#`
 `config>system>time>ntp# multicastclient authenticate`
 `config>system>time>ntp# no shutdown`

The following example shows NTP enabled with the multicastclient command configured.

```
A:ALA-12>config>system>time# info
```

```
-----
server 192.168.15.221
multicastclient
no shutdown
-----
A:ALA-12>config>system>time##
```

NTP-Server

The **ntp-server** command configures the node to assume the role of an NTP server. Unless the server command is used this node will function as an NTP client only and will not distribute the time to downstream network elements. If authentication is specified in this command, the NTP server requires client packets to be authenticated based on the key received in the client request.

CLI Syntax: config>system>time>ntp
 ntp-server [authenticate]

Example: config>system>time>ntp#
 config>system>time>ntp# ntp-server
 config>system>time>ntp# no shutdown

The following example shows NTP enabled with the ntp-server command configured.

```
A:sim1>config>system>time>ntp# info
-----
no shutdown
ntp-server
-----
A:sim1>config>system>time>ntp#
```

Peer

Configuration of an NTP peer configures symmetric active mode for the configured peer. Although any system can be configured to peer with any other NTP node, it is recommended to configure authentication and to configure known time servers as their peers. Use the **no** form of the command to remove the configured peer.

CLI Syntax: config>system>time>ntp
 peer ip-address [version version] [key-id key-
 id]
 [prefer]

Example: config>system>time>ntp#
 config>system>time>ntp# peer 192.168.1.1 key-id 1

```
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the peer command configured.

```
A:sim1>config>system>time>ntp# info
-----
no shutdown
peer 192.168.1.1 key-id 1
-----
A:sim1>config>system>time>ntp#
```

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 ten NTP servers can be configured.

CLI Syntax: config>system>time>ntp
 server *ip-address* [*key-id key-id*] [*version*
 version] [*prefer*]

Example: config>system>time>ntp#
 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#
```

5.18.1.3.5 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
```

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#
config>system>time>sntp# broadcast-client
config>system>time>sntp# no shutdown
```

The following example shows SNTP enabled with the **broadcast-client** command enabled.

```
A:ALA-12>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
-----
A:ALA-12>config>system>time#
```

Server-address

The **server-address** command configures an SNTP server for SNTP unicast client mode.

CLI Syntax:

```
config>system>time>sntp#
```



```
config>system>time>sntp# server-address ip-address
                        version version-number] [normal|preferred] [interval
                        seconds]
```

Example:

```
config>system>time>sntp#
config>system>time# server-address 10.10.0.94 version 1
preferred interval 100
```

The following example shows SNTP enabled with the **server-address** command configured.

```
A:ALA-12>config>system>time# info
-----
sntp
server-address 10.10.0.94 version 1 preferred interval 100
no shutdown
exit
dst-zone PT start-date 2006/04/04 12:00 end-date 2006/10/25 12:00
zone GMT
-----
A:ALA-12>config>system>time#
```

5.18.1.3.6 CRON

CRON provides various time and date scheduling functions. Configuration notes for the CRON schedule are provided below.

Schedule

The schedule function configures the type of schedule to run, including one-time only (oneshot), periodic or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute and interval (seconds). If end-time and interval are both configured, whichever condition is reached first is applied.

Example:

```
config>system>cron# schedule test2
config>system>cron>sched# day-of-month 17
config>system>cron>sched# end-time 2007/07/17 12:00
config>system>cron>sched# minute 0 15 30 45
config>system>cron>sched# weekday friday
config>system>cron>sched# shut
```

The following example schedules a script named “test2” to run every 15 minutes on the 17th of each month and every Friday until noon on July 17, 2007:

```
*A:SR-3>config>system>cron# info
-----
```

```
schedule "test2"
shutdown
day-of-month 17
minute 0 15 30 45
weekday friday
end-time 2007/07/17 12:00
exit
-----
*A:SR-3>config>system>cron#
```

5.18.1.4 ANCP Enhancements

Persistence is available for subscriber's ANCP attributes and is stored on the on-board compact flash card. ANCP data will stay persistence during an ISSU as well as nodal reboots. During recovery, ANCP attributes are first restored fully from the persistence file, and incoming ANCP sessions are temporarily on hold. Afterwards, new ANCP data can overwrite any existing values. This new data is then stored into the compact flash in preparation for the next event.

5.18.2 Configuring Synchronization and Redundancy

- [Configuring Persistence](#)
- [Configuring Synchronization](#)
- [Configuring Manual Synchronization](#)
- [Forcing a Switchover](#)
- [Configuring Synchronization Options](#)
- [Configuring Multi-Chassis Redundancy for LAG](#)

5.18.2.1 Configuring Persistence

The following example shows subscriber management system persistence command usage for the 7450 ESS and 7750 SR:

Example:

```
config>system# persistence
config>system>persistence# subscriber-mgmt
config>system>persistence>sub-mgmt# description
"cf3:SubMgmt-Test"
config>system>persistence>sub-mgmt# location cf3:
config>system>persistence>sub-mgmt# exit
```

```
A:ALA-12>config>system>persistence# info
-----
subscriber-mgmt
  description "cf3:SubMgmt-Test"
  location cf1:
exit
-----
A:ALA-12>config>system>persistence#
```

5.18.2.2 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 CPM card.

CLI Syntax:

```
admin>redundancy
synchronize {boot-env|config}
config>system
switchover-exec file-url
```

5.18.2.3 Configuring Manual Synchronization

Note that automatic synchronization can be configured in the **config>system>synchronization** context.

CLI Syntax:

```
admin
redundancy
  synchronize {boot-env|config}
```

Example:

```
admin>redundancy# synchronize config
```

The following shows the output shown during a manual synchronization:

```
A:ALA-12>admin# synchronize config

Syncing configuration.....

Syncing configuration.....Completed.
A:ALA-12#
```

5.18.2.4 Forcing a Switchover

The **force-switchover now** command forces an immediate switchover to the standby CPM card.

CLI Syntax: admin>redundancy
 force-switchover [now]

Example: admin>redundancy# force-switchover now

```
A:ALA-12# admin redundancy force-switchover now
A:ALA-12#
Resetting...
?
```

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

5.18.2.5 Configuring Synchronization Options

Network operators can specify the type of synchronization operation to perform between the primary and secondary CPMs after a change has been made to the configuration files or the boot environment information contained in the boot options file (BOF).

Use the following CLI to configure the boot-env option:

CLI Syntax: config>system
 synchronize {boot-env|config}

Example: config>system# synchronize boot-env

The following example shows the configuration:

```
A:ALA-12>config>system# synchronize boot-env
A:ALA-12>config>system# show system synchronization
=====
Synchronization Information
=====
Synchronize Mode       : Boot Environment
Synchronize Status     : No synchronization
Last Config Sync Time  : 2006/06/27 06:19:47
Last Boot Env Sync Time : 2006/06/27 06:19:47
=====
A:ALA-12>config>system#
```

Use the following CLI to configure the config option:

CLI Syntax: config>system

```
synchronize {boot-env|config}
```

Example: config>system# synchronize config

The following example shows the configuration.

```
A:ALA-12>config>system# synchronize config
A:ALA-12>config>system# show system 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
=====
A:ALA-12>config>system#
```

5.18.3 Configuring Multi-Chassis Redundancy for LAG

When configuring associated LAG ID parameters, the LAG must be in access mode and LACP must be enabled.

Use the CLI syntax shown below 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 duration
        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
    no shutdown
    source-address ip-address
    sync
        igmp
        igmp-snooping
        pim-snooping [sap]
        port [port-id | lag-id] [sync-tag sync-
            tag]
            range encap-range sync-tag sync-tag
```

```
no shutdown
srrp
sub-mgmt
```

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 example shows the configuration:

```
A:ALA-48>config>redundancy# info
-----
multi-chassis
peer 10.10.10.2 create
description "Mc-Lag peer 10.10.10.2"
mc-lag
no shutdown
exit
no shutdown
exit
exit
-----
A:ALA-48>config>redundancy#
```

5.18.4 Configuring Mixed Mode

The 7450 mixed mode feature allows a 7450 ESS-7 or ESS-12 chassis to utilize 7750 IOM3-XPBs, MDAs, and IMMs to enable 7750 SR capabilities on the associated slots. This allows features such as multicast routing, VPRN and IPv6 support as well as others to be enabled on existing 7450 systems.

The following are mixed-mode requirements:

- SR capabilities (for example, IP-VPNs, IPv6 routing and multicast routing) can only be associated with interfaces on 7750 IOM3-XPBs, MDAs, and IMMs

- Network interface ports must be located 7750 IOM3-XP or IMMs
- Only the 7750 SR IOM3-XP, 7750 SR MDAs, or 7750 SR IMMs can be used in the 7450 ESS slots with SR capabilities enabled.



Note:

- ESM for IPv6 must run on IOM-3 or IMM hardware only, not on IOM or IOM-2, because the IOM and IOM2 data planes are not capable of routing incoming traffic to the IPv6 ESM hosts.
- The scaling limits are still defined by the chassis mode. That means only 16k IPv6 ESM subscribers (limited by the ARP scale of chassis mode A).

5.18.4.1 Enabling Mixed Mode on a 7450 System

To configure mixed mode support, 7750 SR IOM3-XP, 7750 MDAs, or 7750 SR IMMs must be installed in a 7450 ESS-7 or ESS-12 router that is running OS 8.0 or later. All network interfaces must be migrated to ports on the 7750 SR cards.

The mixed mode state is then enabled by using the **mixed-mode-upgrade** command:

CLI Syntax: `mixed-mode-upgrade slot-list`

This tool will take a list of slots that should have 7750 SR cards installed. The command then checks to ensure that all network interfaces are located on ports on these slots and that they are all 7750 SR cards. It then enables the **mixed-mode** state at the system level and changes the **capability** setting for the specified slots to **sr**.

At this point the 7450 ESS system is operating in a mixed mode state and supported features and services can now be configured on the slots with SR capabilities enabled.

Once in mixed mode use the **capability** command to configure slots for SR capabilities:

CLI Syntax: `config>card>capability [sr | ess]`

Slots using 7750 SR-capable cards will have to have 7750 SR capability enabled on all slots with 7750 SR IOM3s and IMMs, as well as **mixed-mode** at the system level.

See [Table 42](#) for a description of mixed-mode support.



Note: This table is not intended to be exhaustive, but to provide examples to illustrate the basic principle of mixed versus non-mixed mode operation.

Table 42 Mixed-Mode Support

Feature	7450 ESS Standard Mode	7450 ESS Mixed Mode (Limited to 7750 SR IOM3/ IMM)
Full IES Support	Limited IES support	Yes
Full VPRN Support	No	Yes
BGP for routing (all address families)	No	Yes
IPv6 routing: IPv6 routing (Unicast and Multicast) 6PE 6VPE (IPv6 VPRN)	No	Yes
IP Multicast routing and forwarding Protocols: PIM, MSDP and IGMP mVPN P2MP LSP support	No	Yes
Spoke termination on L3 (IES/VPRN) interfaces	No	Yes
TPSDA IPv4 & v6 Routed subscriber management support PPPoE support SRRP Routed subscriber management for wholesale	No	Yes
IP Mirroring	No	Yes

5.18.5 Configuring Power Supply Parameters

The following is an example for the 7750 SR and 7950 XRS:


```
A:ALA-12>config>system# info
```

```
-----  
..  
    name "ALA-12"  
    contact "Fred Information Technology"  
    location "Bldg.1-floor 2-Room 201"  
    clii-code "abcdefg1234"  
    coordinates "N 45 58 23, W 34 56 12"  
    power-supply 1 dc  
    power-supply 2 dc  
    lacp-system-priority 1  
    sync-if-timing  
        begin  
        ref-order ref1 ref2 bits  
        ref1  
            shutdown  
        exit  
        ref2  
            shutdown  
        exit  
        bits  
            shutdown  
            interface-type dsl esf  
        exit  
        commit  
    exit  
..
```

The following is an example for the 7450 ESS:

```
-----  
A:ALA-12>config>system# info
```

```
-----  
..  
    name "ALA-12"  
    contact "Fred Information Technology"  
    location "Bldg.1-floor 2-Room 201"  
    clii-code "abcdefg1234"  
    coordinates "N 45 58 23, W 34 56 12"  
    power-supply 1 dc  
    power-supply 2 dc  
    lacp-system-priority 1  
    sync-if-timing  
        begin  
        ref-order ref1 ref2 bits  
        ref1  
            shutdown  
        exit  
        ref2  
            shutdown  
        exit  
        bits  
            shutdown  
            interface-type dsl esf  
        exit  
        commit  
..
```

```

        exit
    ..
-----
A:ALA-12>config>system#

```

5.18.6 Configuring ATM System Parameters

The ATM context configures system-wide ATM parameters for the 7750 SR.

```
CLI Syntax: config>system#
            atm
            atm-location-id location-id
            oam
            loopback-period period
            retry-down retries
            retry-up retries
```

```
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
                config>system>atm# oam
                config>system>atm>oam# loopback-period 30
                config>system>atm>oam# retry-down 5
                config>system>atm>oam# retry-up 3
                config>system>atm>oam# exit
```

The following example shows the ATM configuration.

```
A:ALA-12>config>system>atm# info
-----
      atm-location-id 03:00:00:00:00:00:00:00:00:00:00:00:00:00:00
      oam
          retry-up 3
          retry-down 5
          loopback-period 30
      exit
-----
A:ALA-12>config>system>atm#
```

5.18.7 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, assume the **config-backup count** is set to **5** and the configuration file is called *xyz.cfg*. When a **save** command is executed, the file *xyz.cfg* is saved with a .1 extension. 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 SF/CPMSF/CPM 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.

```
A:ALA-12>config>system>time# info
#-----
echo "System Configuration"
#-----
      name "ALA-12"
      contact "Fred Information Technology"
      location "Bldg.1-floor 2-Room 201"
      clii-code "abcdefg1234"
      coordinates "N 45 58 23, W 34 56 12"
      config-backup 7
...
#-----
A:ALA-12>config>system>time#
```

5.18.8 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://
test:test@192.168.xx.xxx/./
fail.cfg
config>system# boot-good-exec ftp://
test:test@192.168.xx.xxx/./
ok.cfg
```

The following example shows the command output:

```
A:ALA-12>config>system# info
#-----
echo "System Configuration"
#-----
    name "ALA-12"
    contact "Fred Information Technology"
    location "Bldg.1-floor 2-Room 201"
    cli-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"
    power-supply 1 dc
    power-supply 2 dc
    lacp-system-priority 1
    sync-if-timing
    begin
    ref-order ref1 ref2 bits
    ..
#-----
A:ALA-12>config>system#
```

5.18.8.1 Show Command Output and Console Messages

The **show>system>information** command shows 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.

The following is an example for the 7750 SR:

```
ALA-12>config>system# show system information
=====
System Information
=====
System Name           : ALA-12
System Contact        : Fred Information Technology
System Location       : Bldg.1-floor 2-Room 201
System Coordinates    : N 45 58 23, W 34 56 12
System Up Time        : 1 days, 04:59:33.56 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f000000000467ff00
SNMP Max Message Size : 1500
SNMP Admin State      : Disabled
SNMP Oper State       : Disabled
SNMP Index Boot Status : Not Persistent

BOF Source            : cfl:
Image Source          : primary
Config Source         : primary
Last Booted Config File: ftp://test:test@192.168.xx.xxx/./12.cfg
Last Boot Cfg Version : THU MAR 04 22:39:03 2004 UTC
Last Boot Config Header: # TiMOS-L-14.0.B1-217 boot/
i386 Nokia 7750 SR Copyright (c)
                        2000-2016 Nokia.
                        # All rights reserved. All use subject to applicable licens
e
                        agreements.
                        # Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /
rel14.0/b1/B1-217/panos/main

Last Boot Index Version: N/A
Last Boot Index Header : N/A
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: Yes
Time Last Modified     : 2004/03/06 03:30:45
Max Cfg/BOF Backup Rev : 7
Cfg-OK Script          : ftp://test:test@192.168.xx.xxx/./ok.cfg
Cfg-OK Script Status   : not used
Cfg-Fail Script        : ftp://test:test@192.168.xx.xxx/./fail.cfg
Cfg-Fail Script Status : not used

Management IP Addr     : 192.168.xx.xxx/20
DNS Server             : 192.168.1.254
DNS Domain             : eng.timetra.com
BOF Static Routes      :
```

```

      To                Next Hop
      172.22.184.0/22    192.168.1.251
ICMP Vendor Enhancement: Disabled
ATM Location ID       : 01:00:00:00:00:11:00:00:00:00:00:00:00:00:00:00
=====
ALA-12>config>system#

```

When executing a post-boot configuration extension file, status messages are output to the **CONSOLE** screen prior to the “Login” prompt.

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/./l2.cfg' ...
System Configuration
Log Configuration
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./l2.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-L-14.0.B1-217 boot/i386 Nokia 7750 SR Copyright (c) 2000-2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /rel14.0/b1/B1-217/panos/main

```

Login:

5.19 System Timing

In the event that network timing is required for the synchronous interfaces in the router, a timing subsystem is utilized to provide a clock to all synchronous interfaces within the system.

This section describes the commands used to configure and control the timing subsystem.

Use the CLI syntax shown below to:

- [Edit Mode](#)
- [Configuring Timing References](#)

- [Using the Revert Command](#)
- [Other Editing Commands](#)
- [Forcing a Specific Reference](#)

5.19.1 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 shows when the you try to modify **sync-if-timing** parameters without entering the keyword **begin**.

```
A:ALA-12>config>system>sync-if-timing>ref1# source-port 2/1/1
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 2/1/1
A:ALA-12>config>system>sync-if-timing>ref1#
```

5.19.2 Configuring Timing References

Use the following CLI syntax to configure timing reference parameters. The source port specified for **ref1** and **ref2** is dependent on the router model type and chassis slot. Please refer to the details in the specific command descriptions.

The following shows a timing reference configuration example for the router:

```
ALA-12>config>system>sync-if-timing# info
-----
ref-order ref2 ref1 bits
ref1
    source-port 3/1/1
    no shutdown
exit
ref2
    source-port 6/1/2
    no shutdown
exit
bits
    interface-type dsl esf
```

```
no shutdown
exit
-----
ALA-12>config>system>sync-if-timing#
```

5.19.3 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. When the failed reference becomes operational, it is eligible for selection.

When mode is non-revertive, a failed clock source is not selected again. If a node would enter holdover due to the references being in previous failed state, then the node will select one of the previously failed references rather than going into holdover.

CLI Syntax: `config>system>sync-if-timing
 revert`

If the current reference goes offline or becomes unstable the revert command allows the clock to revert to a higher-priority reference.

When revertive switching enabled a valid timing reference of the highest priority is used. If a reference with a higher priority becomes valid, a reference switch over to that reference is initiated. If a failure on the current reference occurs, the next highest reference takes over.

If non-revertive switching is enabled, the valid active reference always remains selected even if a higher priority reference becomes available. If the active reference becomes invalid, a reference switch over to a valid reference with the highest priority is initiated. The failed reference is eligible for selection once it becomes operational.

CLI Syntax: `config>system>sync-if-timing
 no revert`

5.19.4 Other Editing Commands

Other editing commands include:

- **commit** — This command saves changes made to the timing references during a session. Modifications are not persistent across system boots unless this command is entered.

- **abort** — This command discards changes that have been made to the timing references during a session.

CLI Syntax: `config>system>sync-if-timing
abort
commit`

5.19.5 Forcing a Specific Reference

The debug sync-if-timing force-reference command should only be used to test and debug problems. Network synchronization problems may appear if network elements are left with this manual override setting. Once the system timing reference input has been forced, it may be cleared using the **no force-reference** command.

You can force the CPM clock to use a specific input reference using the **force-reference** command.

When the command is executed, the CPM clock on the active CPM immediately switches its input reference to that specified by the command. If the specified input is not available (shutdown), or in a disqualified state, the CPM clock shall use the next qualified input reference based on the selection rules.

This command also affects the BITS output port. If the BITS output port selection is set to line-reference and the reference being forced is not the BITS input port, then the system uses the forced reference to generate the signal out the BITS output port. If the BITS output port selection is set to internal-clock, then the system uses the output of the CPM clock to generate the signal for the BITS output port.

On a CPM activity switch, the force command is cleared and normal reference selection is determined.

Debug configurations are not saved between reboots.

CLI Syntax: `debug>sync-if-timing
force-reference {ref1 | ref2 | bits}

debug>sync-if-timing# force-reference`

The 7750 SR-c4 has two BITS input ports on the CFM. The force reference command on this system allows the selection of the specific port.

CLI Syntax: `debug>sync-if-timing
force-reference {ref1 | ref2 | bits1 | bits2}`

5.20 Configuring System Monitoring Thresholds

5.20.1 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 be created to record the occurrence of the event. It can also specify whether an SNMP notification (trap) be generated for the event. There are two notifications for threshold crossing events, a rising alarm and a falling alarm.ping-address

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the 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 event logs and that is distributed to whatever log destinations are configured: console, session, memory, file, syslog, or SNMP trap destination. The 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 function. 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 and alarms and compact flash usage warnings and alarms.

To create events, use the following CLI:

```
CLI Syntax: config>system>thresholds# cflash-cap-warn cf1-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>thresh# rmon

config>system>thresh>rmon# event 5 both description
"alarm testing" owner "Timos CLI"
```

The following example shows the command output:

```
A:ALA-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:ALA-49>config>system>thresholds#
```

5.20.2 System Alarm Contact Inputs

Alarm contact inputs are physical input pins on the Alarms Interface Port of the CPM that allow the operator to monitor and report changes in external environmental conditions. In a remote or outdoor deployment, alarm inputs typically allow an operator to detect conditions such as whether a door is open or closed, an air conditioner fault has occurred, and so on.

There are four input pins, each of which can be configured with an associated severity level and normally open/normally closed state. When an input pin changes state, the router can generate log events and raise facility alarms.

There is a separate log event for each pin (for example, CHASSIS event 3003 `tmnxSasAlarminput3StateChanged` for input pin 3). The severity level of input pin 3 is controlled by configuring the severity level of the associated log event (using the **configure log event-control** command).

There is also a single +24VDC power output pin on the Alarms Interface Port of the CPM that can be used to supply power for the alarm inputs.

The alarm inputs can be powered in one of two ways:

- using the +24Vdc power output pin
- using an external power source

The power output pin provided on the CPM is monitored, and the router can report when the power source fails.

If using an external power source for the alarm inputs, then it is recommended that the **normal-state closed** configuration be used so that a failure of the external power source will trigger all the alarm pins to detect a change of state. If **normal-state open** is used, a failure of the external power source will not generate any notifications and the alarm input pins will no longer operate correctly.

5.21 Configuring LLDP

The following output shows LLDP defaults:

```
A:testSr1>config>system>lldp# info detail
-----
no tx-interval
no tx-hold-multiplier
no reinit-delay
no notification-interval
no tx-credit-max
no message-fast-tx
no message-fast-tx-init
no shutdown
-----
A:testSr1>config>system>lldp#
```

The following example shows an LLDP port configuration:

```
*A:ALA-48>config>port>ethernet>lldp# info
-----
dest-mac nearest-bridge
admin-status tx-rx
tx-tlvs port-desc sys-cap
tx-mgmt-address system
exit
-----
*A:ALA-48>config>port>ethernet>lldp#
```

The following example shows a global system LLDP configuration:

```
A:ALA-48>config>system>lldp# info
-----
```

```
tx-interval 10
tx-hold-multiplier 2
reinit-delay 5
notification-interval 10
-----
A:ALA-48>config>system>lldp#
```


5.22 System Command Reference

5.22.1 Command Hierarchies

5.22.1.1 Configuration Commands

- [System Information Commands](#)
- [System Alarm Contact Input Commands](#)
- [System Threshold Alarm Commands](#)
- [Mixed Mode Configuration Commands](#)
- [Persistence Commands](#)
- [PTP Commands](#)
- [System Time Commands](#)
- [Cron Commands](#)
- [Script Control Commands](#)
- [System Synchronization Commands](#)
- [System Administration \(Admin\) Commands](#)
- [High Availability \(Redundancy\) Commands](#)
- [LLDP System Commands](#)
- [LLDP Ethernet Port Commands](#)
- [Optical Extension Shelf \(OES\) Commands](#)
- [System Router Instance Commands](#)

5.22.1.2 System Information Commands

```

config
— system
— atm
— atm-location-id location-id
— no atm-location-id
— oam
— loopback-period period
— no loopback-period
— retry-down retries
— no retry-down
— retry-up retries
— no retry-up
— boot-bad-exec file-url
— no boot-bad-exec
— boot-good-exec file-url
— no boot-good-exec
— chassis-mode chassis-mode [force]
— clli-code clli-code
— no clli-code
— config-backup count
— no config-backup
— contact contact-name
— no contact
— coordinates coordinates
— no coordinates
— dns
— address-pref {ipv4-only | ipv6-first}
— no address-pref
— dnssec
— ad-validation {fall-through | drop}
— [no] ad-validation
— [no] enable-icmp-vse
— ip
— [no] enforce-unique-if-index
— lacp-system-priority lacp-system-priority
— no lacp-system-priority
— load-balancing
— [no] l4-load-balancing
— lsr-load-balancing {lbl-only | lbl-ip | ip-only | eth-encap-ip}
— no lsr-load-balancing
— [no] mc-enh-load-balancing
— [no] service-id-lag-hashing
— [no] system-ip-load-balancing
— location location
— no location
— name system-name
— no name
— port-topology
— port port-id to port-id [create]
— no port port-id
— power-supply power-supply-id type

```


- **satellite**
 - **eth-sat** *sat-id* [create]
 - **no eth-sat**
 - **description** *description-string*
 - **no description**
 - **mac-address** *mac-address*
 - **no mac-address**
 - **sat-type** *sat-type*
 - **no sat-type**
 - [no] **software-repository** *repository-name*
 - [no] **shutdown**
 - [no] **sync-e**
- **software-repository** *repository-name* [create]
- **no software-repository** *repository-name*
 - **description** *description-string*
 - **no description**
 - **primary-location** *file-url*
 - **no primary-location**
 - **secondary-location** *file-url*
 - **no secondary-location**
 - **tertiary-location** *file-url*
 - **no tertiary-location**

5.22.1.3 System Alarm Contact Input Commands

- ```
config
— system
— alarm-contact-in-power {on | off}
— alarm-contact-input input-pin-number
— clear-alarm-msg message-string
— no clear-alarm-msg
— description description-string
— no description
— normal-state {open | closed}
— [no] shutdown
— trigger-alarm-msg message-string
— no trigger-alarm-msg
```

### 5.22.1.4 System Threshold 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-alarm-pct** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *rmon-event-type*] [**startup-alarm** *alarm-type*]
- **no cflash-cap-alarm-pct** *cflash-id*
- **cflash-cap-warn** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *rmon-event-type*] [**startup-alarm** *alarm-type*]
- **no cflash-cap-warn** *cflash-id*
- **cflash-cap-warn-pct** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *rmon-event-type*] [**startup-alarm** *alarm-type*]
- **no cflash-cap-warn-pct** *cflash-id*
- **kb-memory-use-alarm** **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *rmon-event-type*] [**startup-alarm** *alarm-type*]
- **no kb-memory-use-alarm**
- **kb-memory-use-warn** **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *rmon-event-type*] [**startup-alarm** *alarm-type*]
- **no kb-memory-use-warn**
- **memory-use-alarm** **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [**rmon-event-type** *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** *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*

5.22.1.5 Mixed Mode Configuration Commands



Note: The commands listed in this section apply only to the 7450 ESS.

```
config
  — card
    — capability {sr | ess} [now]

config
  — system
    — [no] mixed-mode
```

5.22.1.6 Persistence Commands



Note: The commands in this section only apply to the 7750 SR.

```
config
  — system
    — persistence
      — ancp
        — description description-string
        — no description
        — location cflash-id
        — no location
      — application-assurance
        — description description-string
        — no description
        — location cflash-id
        — no location
      — dhcp-server
        — description description-string
        — no description
        — location cflash-id
        — no location
      — nat-port-forwarding
        — description description-string
        — no description
        — location cflash-id
        — no location
      — options
        — dhcp-lease-time-threshold [days days] [hrs hours] [min minutes] [sec seconds]
        — no dhcp-lease-time-threshold
      — python-policy-cache
        — description description-string
        — no description
        — location cflash-id
        — no location
      — subscriber-mgmt
        — description description-string
        — no description
        — location cflash-id
        — no location
```

5.22.1.7 PTP Commands



Note: The commands in this section apply to the 7450 ESS and 7750 SR, except the 7750 SR-1e, 7750 SR-2e, and 7750 SR-3e.

```

config
  — system
    — ptp
      — anno-rx-timeout count
      — no anno-rx-timeout
      — clock-type boundary
      — clock-type ordinary {master | slave}
      — domain domain-value
      — no domain
      — local-priority priority
      — log-anno-interval log-interval
      — no log-anno-interval
      — network-type {sdh | sonet}
      — peer ip-address [create]
      — no peer ip-address
        — log-sync-interval log-interval
        — no log-sync-interval
        — local-priority local-priority
        — [no] shutdown
      — peer-limit limit
      — no peer-limit
      — port port-id [create]
      — no port port-id
        — address {01:1b:19:00:00:00|01:80:c2:00:00:0e}
        — local-priority priority
        — log-delay-interval log-interval
        — no log-delay-interval
        — log-sync-interval log-interval
        — no log-sync-interval
        — master-only {true | false}
        — [no] shutdown
      — priority1 priority-value
      — no priority1
      — priority2 priority-value
      — no priority2
      — profile {g8265dot1-2010 | ieee1588-2008 | g8275dot1-2014}
      — [no] shutdown
  
```

5.22.1.8 System Time Commands

```

root
  — admin
  
```

```

— set-time [date] [time]

config
— system
— time
— [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}
— multicast [version version] [key-id key-id]
— no multicast
— multicastclient [authenticate]
— no multicastclient
— ntp-server [authenticate]
— no ntp-server
— [no] peer {ip-address | ipv6-address} [version version] [key-id key-id]
[prefer]
— no peer ip-address
— server {ip-address | ipv6-address | ptp} [key-id key-id] [version version]
[prefer]
— no server ip address
— [no] shutdown
— [no] sntp
— [no] broadcast-client
— server-address ip-address [version version-number] [normal |
preferred] [interval seconds]
— no server-address ip-address
— [no] shutdown
— [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]
— zone std-zone-name | non-std-zone-name [hh [:mm]]
— no zone

```

5.22.1.9 Cron Commands

```

config
— system
— cron
— [no] schedule schedule-name [owner owner-name]
— [no] action action-name [owner owner-name]
— day-of-month {day-number [..day-number] all}
— no day-of-month

```

- **count** *number*
- **no count**
- **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-control** *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**

5.22.1.10 Script Control Commands

- ```

config
— system
— script-control
— 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
— script script-name [owner script-owner]
— description description-string
— no description
— location file-url
— no location
— [no] shutdown

```

### 5.22.1.11 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 | eec1 | sec | prc | ssu-a | ssu-b | eec2}
 - **no ql-override**
 - **ssm-bit** *sa-bit*
- **commit**
- **ref-order** *first second [third [fourth]]*
- **no ref-order**
- **ptp**
 - **ql-override** {prs | stu | st2 | tnc | st3e | st3 | eec1 | sec | prc | ssu-a | ssu-b | eec2}
 - **no ql-override**
 - [no] **shutdown**
- **ref1**
 - **bits-interface-type** {ds1 [{esf | sf}] | e1 [{pcm30crc | pcm31crc}]}
 - **no bits-interface-type**
 - **ql-override** {prs | stu | st2 | tnc | st3e | st3 | eec1 | sec | prc | ssu-a | ssu-b | eec2}
 - **no ql-override**
 - [no] **shutdown**
 - **source-bits** *slot/mda*
 - **no source-bits**
 - **source-port** *port-id*
 - **no source-port**
 - **ssm-bit** *sa-bit*
- **ref2**
 - **bits-interface-type** {ds1 [{esf | sf}] | e1 [{pcm30crc | pcm31crc}]}
 - **no bits-interface-type**
 - **ql-override** {prs | stu | st2 | tnc | st3e | st3 | eec1 | sec | prc | ssu-a | ssu-b | eec2}
 - **no ql-override**
 - [no] **shutdown**
 - **source-bits** *slot/mda*
 - **no source-bits**
 - **source-port** *port-id*
 - **no source-port**
 - **ssm-bit** *sa-bit*
- [no] **ql-selection**
- [no] **revert**

5.22.1.12 System Administration (Admin) Commands

```

root
— admin
  — application-assurance
    — upgrade
  — clear-policy-lock
  — debug-save [file-url]
  — disconnect {address ip-address | username user-name | console | telnet | ftp | ssh}
  — display-config [detail | index]
  — [no] enable-tech
  — oes
    — force-switchover chassis-id [now]
    — reboot [now]
  — radius-discovery
    — force-discover [svc-id service-id]
  — reboot [active | standby | upgrade] [hold] [now]
  — redundancy
    — [no] cert-sync
  — save [file-url] [detail] [index]
  — satellite [eth-sat sat-id] reboot [upgrade] [now]
  — satellite [eth-sat sat-id] [sync-boot-env]
  — satellite [eth-sat sat-id] [tech-support file-url]
  — synchronize {boot-env | config}
  — no synchronize
  — synchronize [boot-env | config]
  — tech-support [file-url]
  — ts-location [file-url]

```

5.22.1.13 High Availability (Redundancy) Commands

```

root
— admin
  — display-config [detail | index]
  — redundancy
    — force-switchover [now] [ignore-status]
    — rollback-sync
    — synchronize {boot-env | config}

config
— system
  — switchover-exec file-url
  — no switchover-exec
— redundancy
  — mgmt-ethernet
  — multi-chassis
    — [no] peer ip-address
      — authentication-key [authentication-key | hash-key] [hash | hash2]
      — no authentication-key
      — description description-string

```


-
- **no description**
 - **[no] mc-endpoint**
 - **[no] bfd-enable**
 - **boot-timer** *interval*
 - **no boot-timer**
 - **hold-on-neighbor-failure** *multiplier*
 - **no hold-on-neighbor-failure**
 - **keep-alive-interval** *interval*
 - **no keep-alive-interval**
 - **[no] passive-mode**
 - **[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** *remote-lag-id*] **system-priority** *system-priority* **source-bmac-lsb** *use-lacp-key*
 - **lag** *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *remote-lag-id*] **system-priority** *system-priority* [**source-bmac-lsb** *MAC-Lsb*]
 - **lag** *lag-id* [**remote-lag** *remote-lag-id*]
 - **no lag** *lag-id*
 - **[no] shutdown**
 - **peer-name** *name*
 - **no peer-name**
 - **[no] shutdown**
 - **source-address** *ip-address*
 - **no source-address**
 - **[no] sync**
 - **[no] igmp**
 - **[no] igmp-snooping**
 - **[no] local-dhcp-server**
 - **[no] mc-ring**
 - **[no] mld-snooping**
 - **pim-snooping** [*sap*]
 - **[no] pim-snooping**
 - **port** [*port-id* | *lag-id*] [**sync-tag** *sync-tag*] [**create**]
 - **no port** [*port-id* | *lag-id*]
 - **range** *encap-range* **sync-tag** *sync-tag*
 - **no range** *encap-range*
 - **[no] python**
 - **[no] shutdown**
 - **[no] srrp**
 - **[no] sub-host-trk**
 - **[no] sub-mgmt**
 - **warm-standby**
 - **bgp-multi-homing**
 - **boot-timer** *seconds*
 - **no boot-timer**
 - **site-activation-timer** *seconds*

- no **site-activation-timer**
- **site-min-down-timer** *min-down-time*
- no **site-min-down-timer**
- [no] **cert-sync**
- [no] **rollback-sync**
- **synchronize** {boot-env | config}

5.22.1.14 LLDP System Commands

- ```
configure
 — 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
 — [no] shutdown
 — tx-credit-max count
 — no tx-credit-max
 — tx-hold-multiplier multiplier
 — no tx-hold-multiplier
 — tx-interval interval
 — no tx-interval
```

### 5.22.1.15 LLDP Ethernet Port Commands

- ```
configure
  — port port-id
    — ethernet
      — lldp
        — dest-mac {nearest-bridge | nearest-non-tpmr | nearest-customer}
        — notification {rx | tx | tx-rx | disabled}
        — [no] notification
        — tx-mgmt-address [system]
        — no tx-mgmt-address
        — tx-tlvs [port-desc] [sys-name] [sys-desc] [sys-cap]
        — no tx-tlvs
```

5.22.1.16 Optical Extension Shelf (OES) Commands



Note: OES commands are only applicable to the 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7950 XRS-20, and 7950 XRS-40 routers.

```
configure
  — system
    — oes
      — cf-cache cflash-id
      — chassis chassis-id type type create
      — no chassis
      — description description-string
      — no description
      — fan-speed {normal | maximum}
      — control-communications
        — [no] oes-address ip-address
        — [no] router cpm-vr-name
        — retry-limit retry_num
        — timeout seconds
      — software-repository repository-name
      — no software-repository
```

5.22.1.17 System Router Instance Commands

```
config
  — router [router-instance] [create]
  — no router [router-instance]
```

5.22.2 System Command Reference

5.22.2.1 Generic Commands

shutdown

Syntax	[no] shutdown
Context	config>system>cron>sched config>system>time>ntp config>system>time>sntp

```
config>system>script-control>script-policy
config>system>script-control>script
config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2
config>system>sync-if-timing>ptp
config>system>sync-if-timing>bits>input
config>system>sync-if-timing>bits>output
config>system>persistence>app-assure
config>system>persistence>dhcp-server
config>system>persistence>nat-port-forward
config>system>persistence>python-policy-cache
config>system>persistence>subscriber-mgmt
config>redundancy>multi-chassis>peer
config>redundancy>multi-chassis>peer>mc-lag
config>redundancy>multi-chassis>peer>sync
config>redundancy>mc>peer>mcr>node>cv
config>system>lldp
config>redundancy>multi-chassis>peer>mc-ep
```

Description	<p>This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.</p> <p>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 may be deleted.</p> <p>The no form of this command places the entity into an administratively enabled state.</p>
Default	no shutdown

description

Syntax	description <i>description-string</i> no description
Context	config>system>cron>sched config>system>script-control>script config>system>persistence>anccp config>system>persistence>app-assure config>system>persistence>dhcp-server config>system>persistence>nat-fwd config>system>persistence>sub-mgmt config>system>persistence>dhcp-server config>redundancy>multi-chassis>peer
Description	<p>This command creates a text description stored in the configuration file for a configuration context.</p> <p>The description command associates a text string with a configuration context to help identify the content in the configuration file.</p>

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *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 (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

5.22.2.2 System Information 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

Description This command indicates the location ID for ATM OAM.

Refer to the *7450 ESS, 7750 SR, and 7950 XRS Services Overview Guide* for information about ATM QoS policies and 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

oam

Syntax	oam
Context	config>system>atm
Description	This command configures system-wide ATM parameters.

loopback-period

Syntax	loopback-period <i>period</i> no loopback-period
Context	config>system>atm>oam
Description	This command specifies the number of seconds between periodic loopback attempts on an ATM endpoint that has periodic loopback enabled.
Parameters	<i>period</i> — specifies the time, in seconds, between periodic loopback attempts
Values	1 to 40
Default	10

retry-down

Syntax	retry-down <i>retries</i> no retry-down
Context	config>system>atm>oam
Description	<p>This command specifies the number of OAM loopback attempts that must fail after the periodic attempt before the endpoint will transition to AIS-LOC state.</p> <p>The retry values are configured on a system wide basis and are affective on the next period cycle of any ATM VC SAP using periodic-loopback, if changed. The timeout for receiving a loopback response from the remote peer and declaring the loopack failed is 1 second and is not configurable.</p>
Parameters	<i>retries</i> — specifies the number of failed loopback attempts before an ATM VC goes down
Values	0 to 10 (A zero value means that the endpoint will transition to AIS-LOC state immediately if the periodic loopback attempt fails.)
Default	4

retry-up

Syntax	retry-up <i>retries</i> no retry-up				
Context	config>system>atm>oam				
Description	This command specifies the number of consecutive OAM loopback attempts that must succeed after the periodic attempt before the endpoint will transition the state to up.				
Parameters	<i>retries</i> — specify the number of successful loopback replies before an ATM VC goes up <table> <tr> <td>Values</td><td>0 to 10 (A zero value means that the endpoint will transition to the up state immediately if the periodic loopback attempt succeeds.)</td></tr> <tr> <td>Default</td><td>2</td></tr> </table>	Values	0 to 10 (A zero value means that the endpoint will transition to the up state immediately if the periodic loopback attempt succeeds.)	Default	2
Values	0 to 10 (A zero value means that the endpoint will transition to the up state immediately if the periodic loopback attempt succeeds.)				
Default	2				

boot-bad-exec

Syntax	boot-bad-exec file-url no boot-bad-exec											
Context	config>system											
Description	<p>Use this command to configure a URL for a CLI script to exec 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.</p> <p>The commands are persistent between router (re)boots and are included in the configuration saves (admin>save).</p> <p>Related Commands</p> <p>exec - This command executes the contents of a text file as if they were CLI commands entered at the console.</p>											
Default	no boot-bad-exec											
Parameters	<p><i>file-url</i> — 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.</p> <p>Ipv6-address only applies to the 7750 SR and 7950 XRS.</p> <p>Values</p> <table><tr><td><i>file url</i></td><td><i>local-url remote-url</i></td><td>255 chars max</td></tr><tr><td><i>local-url</i></td><td>[<i>cflash-id</i>]/[<i>file-path</i>]</td><td></td></tr><tr><td><i>remote-url</i></td><td>[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]</td><td></td></tr></table>			<i>file url</i>	<i>local-url remote-url</i>	255 chars max	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]		<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	
<i>file url</i>	<i>local-url remote-url</i>	255 chars max										
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]											
<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]											

	<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6- address</i>]]
	<i>ipv4-address</i>	<i>a.b.c.d</i>
	<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D <i>interface</i> - 32 chars max, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:	

boot-good-exec

Syntax	boot-good-exec <i>file-url</i> no boot-good-exec	
Context	config>system	
Description	Use this command to configure a URL for a CLI script to exec following the success of a boot-up configuration.	
	Related Commands	
	exec - This command executes the contents of a text file as if they were CLI commands entered at the console.	
Default	no boot-good-exec	
Parameters	<i>file-url</i> — specifies the location and name of the file executed following successful completion of the boot-up configuration file execution. When this parameter is not specified, no CLI script file is executed. Ipv6-address only applies to the 7750 SR and 7950 XRS and ipv4-address applies to the 7450 ESS.	

Values

<i>file url</i>	<i>local-url</i> <i>remote-url</i>	255 chars max
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	
<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	
	<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6- address</i>]]
	<i>ipv4-address</i>	<i>a.b.c.d</i>
	<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H

d - [0 to 255]D
interface - 32 chars max, for
link local addresses

cflash-id cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

chassis-mode

Syntax	chassis-mode <i>chassis-mode</i> [force]
Context	config>system
Description	<p>This command configures the chassis scaling and feature set.</p> <p>Note that, if you are in chassis-mode d and configure an IOM type as iom2-20g and then downgrade to chassis-mode a or b (must specify force keyword), a warning appears about the IOM downgrade. In this case, the IOM provisioned type will downgrade to iom-20g-b. Once this is done, the ASAP MDA cannot be configured.</p> <p>The ASAP MDA can only be configured if the iom2-20g IOM type is provisioned and equipped and the chassis mode is configured as a or b.</p> <p>If this is the desired behavior for the 7750 SR, for example, chassis-mode d is configured and IPv6 is running, you can then downgrade to chassis-mode a or b if you want to disable IPv6.</p> <p>For chassis mode d, the default must be changed from the default mode a which assumes the least available features. Mode d enables the new feature sets available with newer generations of IOMs. Chassis mode d supports the P2/Q2/T2-based IOMs products and the extensive queuing/policing/bandwidth. Mode d assumes that the iom3-xp is installed.</p> <p>The force command is not available for chassis-mode d.</p>
Default	chassis-mode a
Parameters	<p><i>chassis-mode</i> — specifies the one of the following chassis modes:</p> <ul style="list-style-type: none">a: This mode corresponds to scaling and feature set associated with iom-20g.b: This mode corresponds to scaling and feature set associated with iom-20g-b.c: This mode corresponds to scaling and feature set associated with iom2-20g (7750 SR only).d: This mode corresponds to scaling and feature set associated with iom3-xp. <p>If the chassis mode is not explicitly provisioned in the configuration file, the chassis will come up in chassis mode a by default. The behavior for the IOMs is described in the following table:</p>

Table 43 Chassis Mode Behavior

IOM	Behavior
iom-20g-b	comes online if provisioned as iom-20g or iom-20g-b
iom2-20g	comes online if provisioned as iom-20g, iom-20g-b or iom2-20g
iom-10g	comes online if provisioned as iom-10g
iom3-xp	comes online if provisioned as iom3-xp

force — forces an upgrade from mode **a** to mode **b** or **d**, or an upgrade from mode **b** to mode **d**

cli-code

Syntax **cli-code** *cli-code*
no cli-code

Context config>system

Description This command creates a Common Language Location Identifier (CLLI) code string for the SR-series router. 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 eleven 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 none — no CLLI codes are configured

Parameters *cli-code* — the 11 character string CLLI code. Any printable, seven bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. If more than 11 characters are entered, the string is truncated. If less than 11 characters are entered the string is padded with spaces.

config-backup

Syntax **config-backup** *count*
no config-backup

Context	config>system
Description	<p>This command configures the maximum number of backup versions maintained for configuration files and BOF.</p> <p>For example, assume the config-backup <i>count</i> is set to 5 and the configuration file is called <i>xyz.cfg</i>. When a save command is executed, the file <i>xyz.cfg</i> is saved with a 1 extension. Each subsequent config-backup command increments the numeric extension until the maximum count is reached.</p> <p><i>xyz.cfg</i> <i>xyz.cfg.1</i> <i>xyz.cfg.2</i> <i>xyz.cfg.3</i> <i>xyz.cfg.4</i> <i>xyz.cfg.5</i> <i>xyz.ndx</i></p> <p>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 <i>xyz.cfg</i> and the index file is created as <i>xyz.ndx</i>. Synchronization between the active and standby CPM is performed for all configurations and their associated persistent index files.</p> <p>The no form of the command returns the configuration to the default value.</p>
Default	config-backup 5
Parameters	<p><i>count</i> — the maximum number of backup revisions</p> <p>Values 1 to 9</p>

contact

Syntax	contact <i>contact-name</i> no contact
Context	config>system
Description	<p>This command creates a text string that identifies the contact name for the device.</p> <p>Only one contact can be configured, if multiple contacts are configured the last one entered will overwrite the previous entry.</p> <p>The no form of the command reverts to default.</p>
Default	none — no contact name is configured
Parameters	<p><i>contact-name</i> — the contact name character string. The string can be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p>

coordinates

Syntax	coordinates <i>coordinates</i> no coordinates
Context	config>system
Description	<p>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.</p> <p>Only one set of coordinates can be configured. If multiple coordinates are configured, the last one entered overwrites the previous entry.</p> <p>The no form of the command reverts to the default value.</p>
Default	none — no coordinates are configured
Parameters	<i>coordinates</i> — the coordinates describing the device location character string. The string may be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), 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.

dns

Syntax	dns
Context	config>system
Description	This command configures DNS settings.
Default	N/A

address-pref

Syntax	address-pref { <i>ipv4-only</i> <i>ipv6-first</i> } no address-pref
Context	config>system>dns
Description	<p>This command configures the DNS address resolving order preference. By default DNS names are queried for A-records only (address-preference is IPv4-only).</p> <p>If the address-preference is set to IPv6-first, the DNS server will be queried for AAAA-records (IPv6) first and if a successful replied is not received, then the DNS server is queried for A-records. IPv6 applies only to the 7750 SR and 7950 XRS.</p>

Default N/A

ad-validation

Syntax	ad-validation {fall-through drop} no ad-validation
Context	config>system>dns>dnssec
Description	<p>This command enables validation of the presence of the AD-bit in responses from the DNS servers, and reports a warning to the SECURITY log if DNSSEC validation was not possible.</p> <p>This command requires either the fall-through or drop parameters be configured. When the fall-through parameter is supplied, the system will allow DNS responses that do not pass DNSSEC validation to be accepted and logged. When the drop parameter is specified, the system will reject and log DNS responses that do not pass DNSSEC validation and the resolution will appear to fail.</p>
Default	disabled
Parameters	<p><i>fall-through</i> — specifies that the DNSSEC validator should allow non-DNSSEC responses to fall-through to permit resolution in case of validation failure</p> <p><i>drop</i> — specifies that the DNSSEC validator should drop non-DNSSEC responses in case of validation failure</p>

enable-icmp-vse

Syntax	[no] enable-icmp-vse
Context	config>system
Description	This command enables vendor specific extensions to ICMP.
Default	no enable-icmp-vse

enforce-unique-if-index

Syntax	[no] enforce-unique-if-index
Context	config>system>ip
Description	This command enables the options to force the creation of IP interface indexes so that they are globally unique across all routing contexts. In addition, the command ensures that any interface created using SNMP also has a system-wide unique IP interface index.

If this command is issued but the system has previously existing interface indexes that conflict, the command will be rejected until all the conflicts are removed. Pre-existing persistency tables should also be removed before enabling this system option.

The **no** form of the command disables this option and returns the system to the default behavior.

Default no enforce-unique-if-index

lacp-system-priority

Syntax	lacp-system-priority <i>lacp-system-priority</i> no lacp-system-priority
Context	config>system
Description	This command configures the Link Aggregation Control Protocol (LACP) system priority on aggregated Ethernet interfaces. LACP allows the operator to aggregate multiple physical interfaces to form one logical interface.
Default	lacp-system-priority 32768
Parameters	<i>lacp-system-priority</i> — specifies the LACP system priority
	Values 1 to 65535

load-balancing

Syntax	load-balancing
Context	config>system
Description	This command enables the load-balancing context to configure the interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.
Default	N/A

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 based on Layer 4 fields. If enabled, the Layer 4 source and destination port fields will be included in hashing calculation for TCP/UDP packets.

The hashing algorithm addresses finer spraying granularity where many hosts are connected to the network.

To address more efficient traffic distribution between network links (forming a LAG group), a hashing algorithm extension takes into account L4 information (that is, src/dst L4-protocol port).

The hashing index can be calculated according to the following algorithm:

```

If [(TCP or UDP traffic) & enabled]
    hash (TCP/UDP ports, IP addresses)
else if (IP traffic)
    hash (IP addresses)
else
    hash (MAC addresses)
endif

```

This algorithm will be used in all cases where IP information in per-packet hashing is included (see LAG and ECMP Hashing in the Interfaces Guide). However, the Layer 4 information (TCP/UDP ports) will not be used for fragmented packets.

Default no l4-load-balancing

lsr-load-balancing

Syntax **lsr-load-balancing** {lbi-only | lbi-ip | ip-only | eth-encap-ip}
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 for spraying labeled IP packets over multiple equal cost paths in ECMP in an LDP LSP and/or over multiple links of a LAG group in all types of LSPs.

The LSR hash routine operates on the label stack and the IP header if a packet is IPv4. An LSR will consider a packet to be IPv4 if the first nibble following the bottom of the label stack is 4. IPv4 is supported only and on IOM-3 and IMMs. IPv6 packets are hashed on label stack only. The hash on label and IPv4 header can be enabled or disabled at the system level only.

Default no lsr-load-balancing

Parameters **lbi-only** — only the label is used in the hashing algorithm
lbi-ip — the IP header is included in the hashing algorithm

ip-only — the IP header is used exclusively in the hashing algorithm

eth-encap-ip — the hash algorithm parses down the label stack (up to 3 labels supported) and once it hits the bottom, the stack assumes Ethernet II non-tagged header follows. At the expected Ethertype offset location, the algorithm checks whether the value present is IPv4/v6 (0x0800 or 0x86DD). If the check passes, the hash algorithm checks the first nibble at the expected IP header location for IPv4/IPv6 (0x0100/0x0110). If the secondary check passes, the hash is performed using IP SA/DA fields in the expected IP header; if any of the checks fail, the label-stack hash is performed.

mc-enh-load-balancing

Syntax	[no] mc-enh-load-balancing
Context	config>system>load-balancing
Description	<p>This command enables enhanced egress multicast load balancing behavior for Layer 3 multicast. When enabled, the router will spray the multicast traffic using as hash inputs from the packet based on lsr-load-balancing, l4-load-balancing and system-ip-load-balancing configurations. That is, an ingress LER or IP PE will spray traffic based on the IP hash criteria: SA/DA + optional Layer 4 port + optional system IP egress LER or LSR - will spray traffic based on label or IP hash criteria outlined above or both based on configuration of lsr-load-balancing, l4-load-balancing, and system-ip-load-balancing.</p> <p>The no form of the command preserves the default behavior for per flow hashing of multicast traffic.</p>
Default	no mc-enh-load-balancing

service-id-lag-hashing

Syntax	[no] service-id-lag-hashing
Context	config>system>load-balancing
Description	<p>This command enables enhanced VLL LAG service ID hashing. This command improves the LAG spraying of VLL service packets and is applied only when both ECMP and LAG hashing are performed by the same router. By default, the ECMP interface and LAG link for all packets on the VLL service are selected based on a direct modulo operation of the service ID. This command enhances distribution and hashes the service ID prior to the LAG link modulo operation when an ECMP link modulo operation is performed.</p> <p>The no form of the command preserves the default behavior of VLL LAG service ID hashing.</p>
Default	no service-id-lag-hashing

system-ip-load-balancing

Syntax	[no] system-ip-load-balancing
Context	config>system>load-balancing
Description	<p>This command enables the use of the system IP address in the ECMP hash algorithm to add a per system variable. This can help guard against cases where multiple routers, in series, will end up hashing traffic to the same ECMP/LAG path.</p> <p>This command is set at a system wide basis, however if certain IOMs do not support the new load-balancing algorithm, they will continue to use the default algorithm. By default, the IPv4 system IP address is used in the hash algorithm. When no IPv4 system IP address is configured, the IPv6 system IP address, when configured, is used in the hash algorithm.</p> <p>The no form of the command resets the system wide algorithm to default.</p>
Default	no system-ip-load-balancing

location

Syntax	location <i>location</i> no location
Context	config>system
Description	<p>This command creates a text string that identifies the system location for the device.</p> <p>Only one location can be configured. If multiple locations are configured, the last one entered overwrites the previous entry.</p> <p>The no form of the command reverts to the default value.</p>
Default	none — no system location is configured
Parameters	<i>location</i> — enter the location as a character string. The string may be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

name

Syntax	name <i>system-name</i> no name
Context	config>system
Description	This command creates a system name string for the device.

For example, system-name parameter ALA-1 for the **name** command configures the device name as ALA-1.

```
ABC>config>system# name "ALA-1"
ALA-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	<i>system-name</i> — enter the system name as a character string. The string may be up to 32 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

switchover-exec

Syntax	switchover-exec <i>file-url</i> no switchover-exec
Context	config>system
Description	<p>This command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CPM card. A switchover can happen because of a fatal failure or by manual action.</p> <p>The CLI script file can contain commands for environment settings, debug (excluding mirroring settings), and other commands not maintained by the configuration redundancy.</p> <p>The following commands are not supported in the switchover-exec file: clear, configure, candidate, oam, tools, oam, ping, traceroute, mstat, mtrace and minfo.</p> <p>When the <i>file-url</i> parameter is not specified, no CLI script file is executed.</p>
Default	no switch-over-exec
Parameters	<i>file-url</i> — specifies the location and name of the CLI script file

port-topology

Syntax	port-topology
Context	config>system
Description	This parameter creates or edits the context to configure intra-node port connections.

Default Disabled

port

Syntax **port** *port-id* **to** *port-id* [**create**]
no port *port-id*

Context config>system>port-topology

Description This command is used for satellites and the Optical Extension Shelf (OES) subsystem. It identifies to the SR OS that there is an internal connection between two ports.

Permitted pairings of the two ports are:

First port	Second port
Router port	Satellite uplink port
Satellite uplink port	Router port
Router port	OES client port
OES client port	Router port

For satellites, this command configures the binding between a host port ID and the satellite uplink from the satellite chassis. The port topology can be configured with the host connected to a satellite uplink or the satellite uplink port connected to the specified host port. Both configurations are supported, as shown in the following examples:

```
*A:Dut-A# configure system port-topology port esat-1/1/u4 to 1/2/2 create
*A:Dut-A# configure system port-topology no port esat-1/1/u4
*A:Dut-A# configure system port-topology port 1/2/2 to esat-1/1/u4 create
*A:Dut-A# configure system port-topology no port 1/2/2
```

For OES, this command configures the internal port connections between the router chassis ports and the OES chassis client ports. One port must be a router port and the other port must be an OES client port.

Example:

```
A:Dut-A# configure system port-topology port 1/5/1 to oes-1/1/c3 create
*
```

The **no** form of the command removes the internal connection.

Default no port port-id

Parameters *port-id* — specifies one port of an internal port connection. These ports can be router ports, Ethernet satellite uplink ports, or OES chassis client ports. Acceptable pairings are defined in the command description.

Values

<i>port-id</i>	(Router port) <i>slot/mda/port</i>		
		<i>slot</i>	The slot number of the card in the chassis. The maximum slot number is platform dependent. See the Install Guides for more information.
		<i>mda</i>	[1 to 2]
		<i>port</i>	[1 to 160] (depending on the MDA type)
	(Ethernet satellite uplink port) <i>esat-id/slot/uport</i>		
		esat	keyword
		<i>id</i>	[1 to 20]
		<i>slot</i>	[1]
		u	keyword for up-link port
		<i>port</i>	[1..4]
	(OES client port) <i>oes-id/slot/cport</i>		
		oes	keyword
		<i>id</i>	[1]
		<i>slot</i>	[1 to 32]
		c	keyword for client port
		<i>port</i>	[1 to 10]

create — specifies the keyword required to create the binding between the two ports

power-supply

Syntax	power-supply <i>power-supply-id type</i>
Context	config>system
Description	This command configures information about the type of power supply used for each power feed connection on the router chassis. The information is used to populate queries made using the show>chassis detail and show>chassis power-supply commands.
Default	N/A
Parameters	<i>power-supply-id</i> — Specifies the power feed connection. Values 1, 2

type — Specifies the type of power source that is connected to the power feed connection.

- Values**
- dc* — Specifies that a single DC power source is connected to the power feed connector.
 - ac single* — Specifies that a single AC power source is connected to the power feed connector.
 - ac multiple* — Specifies that multiple AC power sources are connected to the power feed connector.
 - default* — Reverts the configured information to the default power source type for the chassis.
 - none* — Specifies that no power source is connected to the power feed connector.

satellite

Syntax	satellite
Context	config>system
Description	This command is used to enter the satellite configuration context. Within the satellite context, the administrator can specify the configuration details for a satellite chassis that is hosted by the associated local system.
Default	N/A

eth-sat

Syntax	eth-sat <i>sat-id</i> [create] no eth-sat
Context	config>system>satellite
Description	<p>This command creates the specified Ethernet satellite configuration context. Specific parameters including software-repository, satellite-type, satellite MAC address and sync-e can be configured or modified within this context.</p> <p>The no form of the command deletes the specified Ethernet satellite.</p>
Default	N/A
Parameters	<p><i>sat-id</i> — specifies the satellite ID for the associated Ethernet satellite</p> <p>Values 1 to 20</p> <p>create — the keyword required to create a new Ethernet satellite context</p>

description

Syntax	description <i>description-string</i> no description
Context	config>system>satellite>eth-sat
Description	This command defines a description string that is tied to the associated Ethernet satellite. The no form of the command deletes the associated description string.
Default	no description
Parameters	<i>description-string</i> — ethernet satellite description up to 80 characters in length

mac-address

Syntax	mac-address <i>mac-address</i> no mac-address
Context	config>system>satellite>eth-sat
Description	This command configures the MAC address for the associated Ethernet satellite chassis. This MAC address is used to validate the identity of an Ethernet satellite that attempts to associate with the local host. The no form of the command deletes the MAC address for the associated Ethernet satellite.
Default	N/A
Parameters	<i>mac-address</i> — specifies the MAC address of the associated Ethernet satellite chassis; the MAC should not be a broadcast or multicast MAC. The MAC address should be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

sat-type

Syntax	sat-type <i>sat-type</i> no sat-type
Context	config>system>satellite>eth-sat
Description	This command configures the type of Ethernet satellite variant for the associated satellite chassis. The no form of the command deletes the sat-type configuration.
Default	no sat-type

Parameters	<p><i>sat-type</i> — specifies the Ethernet satellite type. Configuration of the following variants is supported:</p> <p>es24-1gb-sfp — specifies the 24xGE (SFP) + 4x10GE satellite</p> <p>es48-1gb-sfp — specifies the 48xGE (SFP) + 4x10GE satellite</p>
-------------------	---

software-repository

Syntax	[no] software-repository <i>repository-name</i>
Context	config>system>satellite>eth-sat
Description	<p>This command binds the specified software repository to the associated Ethernet satellite. The software repository is used to locate and serve the correct software image to the Ethernet satellite at boot time.</p> <p>The configured software repository is only used when the satellite boots. Changing the software repository for an active satellite does not have an effect until the next time a satellite boots.</p> <p>An Ethernet satellite cannot be booted if there is no software repository defined for it.</p> <p>The no form of the command removes the software repository.</p>
Default	no software-repository
Parameters	<i>repository-name</i> — a string of up to 32 characters that uniquely identifies the software repository

shutdown

Syntax	[no] shutdown
Context	config>system>satellite>eth-sat
Description	<p>This command disables the associated Ethernet satellite.</p> <p>If the associated Ethernet satellite is active, the satellite will not be reset but all satellite client ports will be shut down.</p> <p>If the Ethernet satellite is not active but attempts to associate with the host, the Ethernet satellite chassis will be brought up according to the satellite configuration but all client ports will be shut down.</p> <p>The no form of this command removes the shutdown state and all client ports on active Ethernet satellites will be brought back up.</p>
Default	shutdown

sync-e

Syntax	[no] sync-e
Context	config>system>satellite>eth-sat
Description	<p>This command enables the Ethernet satellite for synchronous Ethernet operation so that the transmit timing of the satellite access ports use the frequency of the host router's central clock.</p> <p>To enable this functionality, both host ports on the router that connect to the U1 and U2 ports of the satellite must be synchronous Ethernet-capable ports.</p> <p>When the Ethernet satellite is configured for synchronous Ethernet, ESMC frames are enabled on the host ports. The SSM code-type used between the host and the satellite should be manually configured on the host ports to match the code-type desired on the satellite client ports. The code-type setting on the host ports does not restrict the code-type used on the satellite client ports, as those may be configured on an individual port basis.</p>
Default	N/A

software-repository

Syntax	software-repository <i>repository-name</i> [create] no software-repository <i>repository-name</i>
Context	config>system
Description	<p>This command creates or deletes an instance of a software repository. The instance is identified by a repository name.</p> <p>A software repository is used to obtain files to upgrade software on certain subsystems of the router (for example, Ethernet satellites).</p> <p>Up to three locations can be specified within a software repository for the router to access files in the repository. The router will first attempt to access the file at the primary location. If the primary location is not configured or the files are not found at the primary location, then the router will attempt to access the files at the secondary location. If the secondary location is not configured or the files are not found at the secondary location, then the router will attempt to access the files at the tertiary location. If the tertiary location is not configured or the files are not found at the tertiary location, then the software repository access will fail.</p> <p>The no form of the command removes the software repository.</p>
Default	N/A
Parameters	<i>repository-name</i> — a string of up to 32 characters that uniquely identifies the software repository

create — keyword required when the software-repository context is first created. Once the context is created, it can be accessed without the **create** keyword.

description

Syntax	description <i>description-string</i> no description
Context	config>system>software-repository
Description	This command defines a description string for the software repository. The no form of the command deletes the associated description string.
Default	no description
Parameters	<i>description-string</i> — software repository description string up to 80 characters in length

primary-location

Syntax	primary-location <i>file-url</i> no primary-location
Context	config>system>software-repository
Description	This command configures the primary location for the files in the software repository. See the software-repository command description for more information. The no form of the command removes the primary location.
Default	N/A
Parameters	<i>file-url</i> — specifies the primary location to be used to access the files in the software repository

Values

<i>file url</i>	<i>local-url</i> <i>remote-url</i>	
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	200 chars maximum, including cflash-id directory length 99 characters maximum each
<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	243 characters maximum directory length 99 characters maximum each
	<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]
	<i>ipv4-address</i>	<i>a.b.c.d</i>

	<i>ipv6-address</i>	<i>x::x::x::x::x::x</i> [- <i>interface</i>] <i>x::x::x::x::d.d.d.d</i> [- <i>interface</i>] <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D <i>interface</i> - 32 characters max, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:	

secondary-location

Syntax	secondary-location <i>file-url</i> no secondary-location	
Context	config>system>software-repository	
Description	This command configures the secondary location for the files in the software repository. See the software-repository command description for more information. The no form of the command removes the secondary location.	
Default	N/A	
Parameters	<i>file-url</i> — specifies the secondary location to be used to access the files in the software repository	
	Values	
	<i>file url</i>	<i>local-url</i> <i>remote-url</i>
	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars maximum, including <i>cflash-id</i> directory length 99 characters maximum each
	<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>] 243 characters maximum directory length 99 characters maximum each
	<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]
	<i>ipv4-address</i>	<i>a.b.c.d</i>
	<i>ipv6-address</i>	<i>x::x::x::x::x::x</i> [- <i>interface</i>] <i>x::x::x::x::d.d.d.d</i> [- <i>interface</i>] <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D <i>interface</i> - 32 characters max, for link local addresses
	<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

tertiary-location

Syntax	tertiary-location <i>file-url</i> no tertiary-location		
Context	config>system>software-repository		
Description	This command configures the tertiary location for the files in the software repository. See the software-repository command description for more information. The no form of the command removes the tertiary location.		
Default	N/A		
Parameters	<i>file-url</i> — specifies the tertiary location to be used to access the files in the software repository		
	Values		
	<i>file url</i>	<i>local-url</i> <i>remote-url</i>	
	<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>]	200 chars maximum, including cflash-id directory length 99 characters maximum each
	<i>remote-url</i>	[{ftp://} <i>login:pswd@remote-locn</i>]/[<i>file-path</i>]	
		243 characters maximum directory length 99 characters maximum each	
		<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> [<i>ipv6-address</i>]]
		<i>ipv4-address</i>	<i>a.b.c.d</i>
		<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D <i>interface</i> - 32 characters max, for link local addresses
	<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:	

5.22.2.3 System Alarm Contact Input Commands

alarm-contact-in-power

Syntax	alarm-contact-in-power {on off}
Context	config>system

Description	This command allows the user to enable a supply of +24V output power on the +24VDC pin of the Alarm Interface Port of the CPM. When enabled, the power supplied through the +24VDC output pin can be used as a source voltage for the alarm contact input pins. The +24VDC output can be used to supply power for monitoring external sensor devices such as cabinet door sensors instead of using an external power source. If users want to use a separate external power source, they should disable the supply of power to the +24VDC output pin by using this CLI command.
Default	alarm-contact-in-power off
Parameters	on — turns on power to the +24VDC output pin of the Alarm Interface Port of the CPM off — turns off power to the +24VDC output pin of the Alarm Interface Port of the CPM

alarm-contact-input

Syntax	alarm-contact-input <i>input-pin-number</i>
Context	config>system
Description	This command provides the context to configure one of four available alarm contact input pins.
Parameters	<i>input-pin-number</i> — identifies the alarm contact input pin Values 1 to 4

clear-alarm-msg

Syntax	clear-alarm-msg <i>message-string</i> no clear-alarm-msg
Context	config>system>alarm-contact-input
Description	This command allows the user to configure a text message for use along with SNMP trap and log event messages that are sent when the system clears an alarm. The system generates the default message "Alarm Input Cleared" if no message is configured. The clear-alarm-msg string is included in the log event when the pin changes to the normal state.
Default	N/A
Parameters	<i>message-string</i> — a printable character string, up to 160 characters in length

description

Syntax	description <i>description-string</i> no description
---------------	---

Context	config>system>alarm-contact-input
Description	This command describes an alarm contact input pin. The description provides an indication of the usage or attribute of the pin. It is stored in the CLI configuration file and helps the user in identifying the purpose of the pin. The description is included in the log event when the pin changes state (the string "Pin x" is used in the log events if no description is configured).
Default	N/A
Parameters	<i>description-string</i> — a printable character string, up to 80 characters in length

normal-state

Syntax	normal-state {open closed}
Context	config>system>alarm-contact-input
Description	<p>This command configures the normal state to be associated with the alarm contact input. When the system detects a transition from the normal state, an alarm is generated. The alarm is cleared when the system detects a transition back to the normal state.</p> <p>Configure the normal state as closed if an external power source is used to power the inputs.</p>
Default	normal-state open
Parameters	<p>open — the normal state is identified as open. When the system detects a transition to the closed state, an alarm is generated. The alarm is cleared when the system detects a transition back to the open state.</p> <p>closed — the normal state is identified as closed. When the system detects a transition to the open state, an alarm is generated. The alarm is cleared when the system detects a transition back to the closed state.</p>

shutdown

Syntax	[no] shutdown
Context	config>system>alarm-contact-input
Description	This command stops tracking the state changes associated with the alarm contact input. The system does not generate or clear the alarms for the alarm contact input, but if an alarm is generated, the system clears the alarm when the shutdown command is executed. The no form of the command starts tracking the state changes associated with the alarm contact input.
Default	shutdown

trigger-alarm-msg

Syntax	trigger-alarm-msg <i>message-string</i> no trigger-alarm-msg
Context	config>system>alarm-contact-input
Description	This command allows the user to configure a text message for use along with SNMP trap and log event messages that are sent when the system generates an alarm. The system generates the default message "Alarm Input Triggered" if no message is configured. The trigger-alarm-msg string is included in the log event when the pin changes from the normal state.
Default	N/A
Parameters	<i>message-string</i> — a printable character string, up to 160 characters in length

5.22.2.4 System Threshold Alarm Commands

thresholds

Syntax	thresholds
Context	config>system
Description	This command enables the context to configure monitoring thresholds.
Default	N/A

cflash-cap-alarm

Syntax	cflash-cap-alarm <i>cflash-id</i> rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [<i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no cflash-cap-alarm <i>cflash-id</i>
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.
Default	N/A
Parameters	<i>cflash-id</i> — the cflash-id specifies the name of the cflash device to be monitored. Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value represents 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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value represents units of 512 bytes.

Values -2147483648 to 2147483647

Default 0

interval *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 cfl-A: rising-threshold 50000000 falling-threshold 49999900
interval 120 rmon-event-type both start-alarm rising
```

cflash-cap-alarm-pct

Syntax	cflash-cap-alarm-pct <i>cflash-id</i> rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [rmon-event-type <i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no cflash-cap-alarm-pct <i>cflash-id</i>
Context	config>system>thresholds
Description	This command enables capacity monitoring of the compact flash specified in this command. The usage is monitored as a percentage of the capacity of the compact flash. 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	<i>cflash-id</i> — the cflash-id specifies the name of the cflash device to be monitored Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B: rising-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal to the falling-threshold value. The threshold value is the percentage of used space versus capacity for the specified compact flash. Values 0 to 100 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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

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 *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-pct cf1-A: rising-threshold 70 falling-  
threshold 60 interval 120 rmon-event-type both start-alarm rising
```

cflash-cap-warn

Syntax	cflash-cap-warn <i>cflash-id</i> rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [<i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no cflash-cap-warn <i>cflash-id</i>
Context	config>system>thresholds
Description	<p>This command enables capacity monitoring of the compact flash specified in this command.</p> <p>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.</p>
Parameters	<p><i>cflash-id</i> — the cflash-id specifies the name of the cflash device to be monitored</p> <p>Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:</p> <p>rising-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal to the falling-threshold value.</p> <p>The threshold value represents units of 512 bytes.</p> <p>Values -2147483648 to 2147483647</p> <p>Default 0</p> <p>falling-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the rising-threshold value.</p> <p>The threshold value represents units of 512 bytes.</p> <p>Values -2147483648 to 2147483647</p> <p>Default 0</p>

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 cfl-B: rising-threshold 2000000 falling-threshold 1999900
interval 240 rmon-event-type trap start-alarm either
```

cflash-cap-warn-pct

Syntax	cflash-cap-warn-pct <i>cflash-id</i> rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [rmon-event-type <i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no cflash-cap-warn-pct <i>cflash-id</i>
Context	config>system>thresholds
Description	This command enables capacity monitoring of the compact flash specified in this command. The usage is monitored as a percentage of the capacity of the compact flash.

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

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

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 *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-pct cf1-B: rising-threshold 70 falling-threshold 60
interval 240 rmon-event-type trap start-alarm either
```

kb-memory-use-alarm

Syntax	kb-memory-use-alarm rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [<i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no kb-memory-use-warn
Context	config>system>thresholds
Description	This command configures memory use, in kilobytes, alarm thresholds. The no form of the command removes the parameters from the configuration.
Default	N/A
Parameters	rising-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

The threshold value represents units of kilobytes.

Default 0

Values -2147483648 to 2147483647

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units of kilobytes.

Default 0

Values -2147483648 to 2147483647

interval *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** — In the case of 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.

Values **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.

Values **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated.

Values **none** — no action is taken

Default **both**

startup-alarm *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, then 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

kb-memory-use-warn

Syntax	kb-memory-use-warn rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [<i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] no kb-memory-use-warn
Context	config>system>thresholds
Description	This command configures memory usage, in kilobytes, for warning thresholds
Default	N/A
Parameters	<p>rising-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.</p> <p>The threshold value represents units of kilobytes.</p> <p>Values -2147483648 to 2147483647</p> <p>Default 0</p> <p>falling-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.</p>

The threshold value represents units of kilobytes.

Values -2147483648 to 2147483647
Default 0

interval *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.

Values **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.

Values **both** — both a entry in the RMON-MIB logTable and a TiMOS logger event are generated

Values **none** — no action is taken

Default **both**

startup-alarm *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, then 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**

memory-use-alarm

Syntax	memory-use-alarm rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] interval <i>seconds</i> [<i>rmon-event-type</i>] [startup-alarm <i>alarm-type</i>] 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 warning.

Default N/A

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

The threshold value represents units of 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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units of bytes.

Values -2147483648 to 2147483647

Default 0

interval *seconds* — specifies the polling period over which the data is sampled and compared with the rising and falling thresholds

The threshold value represents units of bytes.

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 an OS logger entry. The RMON-MIB log table entries can be viewed using the CLI command.

Values **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.

Values **both** — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated

Values **none** — no action is taken

Default **both**

startup-alarm *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, then 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 MemoryUsed 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 compact flash threshold warning.

Default n/a

Parameters	<p>rising-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.</p> <p>Values -2147483648 to 2147483647</p> <p>Default 0</p>
	<p>falling-threshold <i>threshold</i> — 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 will be generated. A single threshold crossing event will also be 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.</p> <p>After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.</p> <p>Values -2147483648 to 2147483647</p> <p>Default 0</p>
	<p>interval <i>seconds</i> — specifies the polling period over which the data is sampled and compared with the rising and falling thresholds</p> <p>Values 1 to 2147483647</p>
	<p>rmon-event-type — specifies the type of notification action to be taken when this event occurs</p> <p>Values log — an entry is made in the RMON-MIB log table for each event occurrence</p> <p>This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command.</p> <p>Values 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.</p> <p>Values both — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated</p> <p>Values none — no action is taken</p> <p>Default both</p>

startup-alarm *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, then 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.

Default **either**
Values **rising, falling, 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 creates 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.

Default N/A

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 alarmTable. 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.

Default	N/A
Parameters	<p><i>rmon-alarm-id</i> — a numerical identifier for the alarm being configured. The number of alarms that can be created is limited to 1200.</p> <p>Values 1 to 65535</p> <p>Default none</p> <p>variable-oid <i>oid-string</i> — 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".</p> <p>The oid-string has a maximum length of 255 characters</p> <p>Default none</p> <p>interval <i>seconds</i> — 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.</p> <p>Values 1 to 2147483647</p> <p>Default none</p> <p>sample-type — specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds</p> <p>Values absolute — specifies that the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval</p> <p>delta — specifies that the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds</p> <p>Default absolute</p> <p>alarm-type — specifies the alarm that may be sent when this alarm is first created</p> <p>If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated.</p>

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.

Default **either**

Values **rising, falling, 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 **rising-event** *rmon-event-id* has a value of zero (0), no associated event exists.

If a **rising-event** *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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value falls below this threshold and reaches less than or equal 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 **falling-event** has a value of zero (0), no associated event exists.

If a **falling-event** is configured, the CLI requires a **falling-threshold** to also be configured.

Values 0 to 65535

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 will be generated. A single threshold crossing event will also be 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 will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Values -2147483648 to 2147483647

Default 0

owner *owner* — the owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be a maximum of 80 characters long.

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 The event command configures an entry in the RMON-MIB event table. 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 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.

Default N/A

Parameters	rmon-event-type — the 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.
Values	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.
Values	both — both an entry in the RMON-MIB logTable and a TiMOS logger event are generated
Values	none — no action is taken
Default	both
	description — The description is a user configurable string that can be used to identify the purpose of this event. This is an optional parameter and can be 80 characters long. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.
	Default an empty string
	owner <i>owner</i> — The owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be a maximum of 80 characters long.
	Default TiMOS CLI

Configuration example:
event 5 rmon-event-type both description "alarm testing" owner "TiMOS CLI"

5.22.2.5 Mixed Mode Configuration Commands

capability

Syntax	capability {sr ess} [now]
Context	config>card

Description	<p>This command sets the desired capability for the associated slot and card. The capability is used along with mixed-mode to enable additional features on certain cards and slots.</p> <p>By default, the capability will be set to that of the base chassis type. To set this to a non-default value, the mixed-mode command must be enabled at the system level.</p> <p>Changing the capability of a slot or card will result in the associated slot being reset. The card-type must first be configured before the capability command can be issued.</p>
Default	capability ess on a 7450 ESS chassis
Parameters	<i>now</i> — This optional keyword can be added to the interactive command to force the command to be executed immediately without further question. If this keyword is not present, then the user will be presented with a question to ensure they understand that as a result of this command, the associated slots will be reset immediately to enable mixed-mode .

mixed-mode

Syntax	[no] mixed-mode
Context	config>system
Description	<p>This command enables chassis support for features with a mixture of IOMs and IMMs.</p> <p>The no form of the command disables mixed mode support.</p>
Default	no mixed-mode

5.22.2.6 Persistence Commands

persistence

Syntax	persistence
Context	config>system
Description	<p>This command enables the context to configure persistence parameters on the system.</p> <p>The persistence feature enables state on information learned through DHCP snooping across reboots to be retained. This information includes data such as the IP address and MAC binding information, lease-length information, and ingress sap information (required for VPLS snooping to identify the ingress interface).</p> <p>If persistence is enabled when there are no DHCP relay or snooping commands enabled, it will simply create an empty file.</p>

Default no persistence

ancp

Syntax **ancp**

Context config>system>persistence

Description This command configures ANCP persistence parameters.

Default N/A

application-assurance

Syntax **application-assurance**

Context config>system>persistence

Description This command configures application assurance persistence parameters.

Default N/A

dhcp-server

Syntax **dhcp-server**

Context config>system>persistence

Description This command configures DHCP server persistence parameters.

Default N/A

nat-port-forwarding

Syntax **nat-port-forwarding**

Context config>system>persistence

Description This command configures NAT port forwarding persistence parameters.

Default N/A

options

Syntax	options
Context	config>system>persistence
Description	This command enables the CLI context to configure persistence options parameters.
Default	N/A

dhcp-lease-time-threshold

Syntax	dhcp-lease-time-threshold [<i>days days</i>] [<i>hrs hours</i>] [<i>min minutes</i>] [<i>sec seconds</i>] no dhcp-lease-time-threshold
Context	config>system>persistence>options
Description	<p>This command configures Dynamic Data Persistence (DDP) compact flash access optimization for DHCP leases.</p> <p>The DHCP lease-time threshold controls the eligibility of a DHCP lease for persistency updates when no data other than the lease expiry time is to be updated. When the offered lease time of the DHCP lease is less than the configured threshold, the lease is flagged to skip persistency updates and will be installed with its full lease time upon a persistency recovery after a reboot.</p> <p>The dhcp-lease-time-threshold command controls persistency updates for DHCPv4 and DHCPv6 leases for a DHCP relay or proxy and DHCPv4 leases for DHCP snooping (enabled with subscriber-mgmt) and a DHCP server (enabled with dhcp-server).</p> <p>The no form of the command disables the DHCP lease time threshold.</p>
Default	no dhcp-lease-time-threshold
Parameters	<p><i>days</i> — the threshold in days</p> <p>Values 0 to 7305</p> <p><i>hours</i> — the threshold in hours</p> <p>Values 0 to 23</p> <p><i>minutes</i> — the threshold in minutes</p> <p>Values 0 to 59</p> <p><i>seconds</i> — the threshold in seconds</p> <p>Values 0 to 59</p>

python-policy-cache

Syntax	python-policy-cache
Context	config>system>persistence
Description	This command configures Python policy cache persistency parameters.
Default	N/A

subscriber-mgmt

Syntax	subscriber-mgmt
Context	config>system>persistence
Description	This command configures subscriber management persistence parameters.
Default	N/A

location

Syntax	location [cf1: cf2: cf3:] no location
Context	config>system>persistence>ancp config>system>persistence>sub-mgmt config>system>persistence>dhcp-server
Description	<p>This command instructs the system where to write the file. The name of the file is: dhcp-persistence.db. On boot the system scans the file systems looking for dhcp-persistence.db, if it finds it starts to load it.</p> <p>In the subscriber management context, the location specifies the flash device on a CPM card where the data for handling subscriber management persistency is stored.</p> <p>The no form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.</p>
Default	no location

5.22.2.7 PTP Commands

ptp

Syntax	ptp
Context	config>system
Description	<p>This command enables the context to configure parameters for IEEE 1588-2008, Precision Time Protocol.</p> <p>This command is only available on the control assemblies that support 1588.</p>

anno-rx-timeout

Syntax	anno-rx-timeout <i>count</i> no anno-rx-timeout
Context	config>system>ptp
Description	<p>This command configures the announceReceiptTimeout value for all peer associations. This defines the number of Announce message intervals that must expire with no received Announce messages before declaring an ANNOUNCE_RECEIPT_TIMEOUT event.</p> <p>The announce-rx-timeout cannot be changed unless PTP is shut down.</p>
Default	anno-rx timeout 3
Parameters	count — the announce packet interval, in log form Values 2 to 10

clock-type

Syntax	clock-type boundary clock-type ordinary { master slave }
Context	config>system>ptp
Description	<p>This command configures the type of clock. The clock-type can only be changed when PTP is shutdown.</p> <p>The clock-type cannot be changed to ordinary master if the PTP reference is no shutdown. In addition, the clock-type cannot be changed to ordinary master if there are peers configured. The clock-type is restricted based on the profile. See the profile command description for the details of the restrictions.</p>

Default	clock-type ordinary slave
Parameters	<p>boundary — The system is a boundary clock, which may be anywhere in the master-slave clock hierarchy. It can obtain timing from a master clock, and provide timing to multiple slave clocks concurrently.</p> <p>ordinary master — The system is a grandmaster clock in the master-slave hierarchy. The system provides timing to multiple slave clocks in the network.</p> <p>ordinary slave — The system is always a slave clock in the master-slave hierarchy. The system derives its timing from one or more master clocks in the network.</p>

domain


Syntax	domain <i>domain</i> no domain						
Context	config>system>ptp						
Description	<p>This command configures the PTP domain.</p> <p>The no form of the command reverts to the default configuration. The default value is dependent upon the configured profile, as detailed below.</p> <p>Note some profiles may require a domain number in a restricted range. It is up to the operator to ensure the value aligns with what is expected within the profile.</p> <p>Domain cannot be changed unless PTP is shutdown. If the PTP profile is changed, the domain is changed to the default domain for the new PTP profile.</p>						
Default	<p>domain 0 — profile ieee1588-2008</p> <p>domain 4 — profile g8265dot1-2010 or</p> <p>domain 24 — profile g8275dot1-2014</p>						
Parameters	<p><i>domain</i> — the PTP domain</p> <table><tr><td>Values</td><td>0 to 255 for ieee1588-2008</td></tr><tr><td></td><td>0 to 255 for g8265dot1-2010</td></tr><tr><td></td><td>24 to 43 for g8275dot1-2014</td></tr></table>	Values	0 to 255 for ieee1588-2008		0 to 255 for g8265dot1-2010		24 to 43 for g8275dot1-2014
Values	0 to 255 for ieee1588-2008						
	0 to 255 for g8265dot1-2010						
	24 to 43 for g8275dot1-2014						

local-priority

Syntax	local-priority <i>priority</i>
Context	config>system>ptp config>system>ptp>peer config>system>ptp>port

Description	<p>This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is relevant when the profile is set to either g8265dot1-2010 or g8275dot1-2014. The parameter is ignored when any other profile is selected.</p> <p>The value 1 is the highest priority and 255 is the lowest priority. The priority of a peer cannot be configured if the PTP profile is ieee1588-2008.</p> <p>For g8265dot1-2010, this parameter configures the priority used to choose between master clocks with the same quality (see G.8265.1 for more details).</p> <p>For g8275dot1-2014, this parameter sets the value of the localPriority associated with the Announce messages received from the external clocks (ptp>peer or ptp>port), or the local clock (PTP). See G.8275.1 for detailed information.</p>
Default	local-priority 128
Parameters	<p><i>local-priority</i> — specifies the value of the local priority</p> <p>Values 1 to 255</p>

log-anno-interval

Syntax	log-anno-interval <i>log-interval</i> no log-anno-interval
Context	config>system>ptp
Description	<p>This command configures the announce message interval used for both unicast and multicast messages.</p> <p>For unicast messages, it 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.</p> <p>For multicast messages, used on PTP Ethernet ports, this configures the message interval used for Announce messages transmitted by the local node.</p> <p>This value also defines the interval between executions of the BMCA within the node.</p> <p>The announce-interval cannot be changed unless the PTP is shut down.</p> <p> Note: In order to minimize BMCA driven reconfigurations, the IEEE recommends that the announce-interval should be consistent across the entire 1588 network.</p>

Default	log-anno-interval 1 (1 packet every 2 seconds) for ieee1588-2008 or log-anno-interval 1 (1 packet every 2 seconds) for g8265dot1-2010 or log-anno-interval -3 (8 packets per second) for g8275dot1-2014
Parameters	<i>log-interval</i> — the announce packet interval, in log form
Values	-3 - 4

network-type

Syntax	network-type { <i>sdh</i> <i>sonet</i> }
Context	config>system>ptp
Description	This command configures the codeset to be used for the encoding of QL values into PTP clockClass values when the profile is configured for G.8265.1. The codeset is defined in Table 1/G.8265.1. This setting only applies to the range of values observed in the clockClass values transmitted out of the node in Announce messages. The router will support the reception of any valid value in Table 1/G.8265.1
Default	network type <i>sdh</i>
Parameters	sdh — specifies the values used on a G.781 Option 1 compliant network sonet — specifies the values used on a G.781 Option 2 compliant network

peer

Syntax	peer <i>ip-address</i> [create] no peer <i>ip-address</i>
Context	config>system>ptp
Description	This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer. Up to 20 remote PTP peers may be configured. The no form of the command deletes the specified peer. If the clock-type is ordinary slave or boundary , and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured and enabled. Peers are created within the routing instance associated with the context of this command. All configured PTP peers must use the same routing instance.
Default	N/A

Parameters	<i>ip-address</i> — the IP address of the remote peer
Values	ipv4-address a.b.c.d

log-sync-interval

Syntax	log-sync-interval <i>log-interval</i> no log-sync-interval
Context	config>system>ptp>peer
Description	<p>This command configures the message interval used for unicast event messages. It defines the message interval for both Sync and Delay_Resp messages that are requested during unicast negotiation to the specific peer. This controls the Sync and Delay_Resp message rate sent from remote peers to the local node. It does not affect the Sync or Delay_Resp packet rate that may be sent from the local node to remote peers. Remote peers may request a Sync or Delay_Resp packet rate anywhere within the acceptable grant range.</p> <p>The log-sync-interval cannot be changed unless the peer is shutdown.</p>
Default	<p>log-sync-interval -6 (64 packets per second) for 1588-2008 or</p> <p>log-sync-interval -6 (64 packets per second) for g8265dot1-2010 or</p> <p>log-sync-interval -4 (16 packets per second) for g8275dot1-2014</p>
Parameters	<i>log-interval</i> — specifies the sync message interval, in log form
Values	[-6 to 0]

shutdown

Syntax	[no] shutdown
Context	config>system>ptp>peer
Description	<p>This command disables or enables a specific PTP peer. Shutting down a peer sends cancel unicast negotiation messages on any established unicast sessions. When shutdown, all received packets from the peer are ignored.</p> <p>If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last enabled peer cannot be shutdown. This prevents the user from having PTP enabled without any peer configured & enabled</p>
Default	no shutdown

peer-limit

Syntax	peer-limit <i>limit</i> no peer-limit				
Context	config>system>ptp				
Description	<p>This command specifies an upper limit to the number of discovered peers permitted within the routing instance. This can be used to ensure that a routing instance does not consume all the possible discovered peers and blocking discovered peers in other routing instances.</p> <p>If it is desired to reserve a fixed number of discovered peers per router instance, then all router instances supporting PTP should have values specified with this command and the sum of all the peer-limit values must not exceed the maximum number of discovered peers supported by the system.</p> <p>If the user attempts to specify a peer-limit, and there are already more discovered peers in the routing instance than the new limit being specified, the configuration will not be accepted.</p>				
Default	no peer-limit				
Parameters	<p><i>limit</i> — specifies the maximum number of discovered peers allowed in the routing instance</p> <table><tr><td>Values</td><td>0 to 50</td></tr><tr><td>Default</td><td>1 (The maximum number of discovered peers supported by the system.)</td></tr></table>	Values	0 to 50	Default	1 (The maximum number of discovered peers supported by the system.)
Values	0 to 50				
Default	1 (The maximum number of discovered peers supported by the system.)				

port

Syntax	port <i>port-id</i> [create] no port <i>port-id</i>
Context	config>system>ptp
Description	<p>This command configures PTP over Ethernet on the physical port. The PTP process shall transmit and receive PTP messages through the port using Ethernet encapsulation (as opposed to UDP/IPv4 encapsulation).</p> <p>The frames are transmitted with no VLAN tags even if the port is configured for dot1q or qinq modes for encap-type. In addition, the received frames from the external PTP clock must also be untagged.</p> <p>There are two reserved multicast addresses allocated for PTP messages (see Annex F IEEE Std 1588™-2008). Either address can be configured for the PTP messages sent through this port.</p> <p>A PTP port may not be created if the PTP profile is set g8265dot1-2010.</p>

If the port specified in the port-id supports 1588 port based timestamping, then a side effect of enabling PTP over Ethernet on the port shall be the enabling of Synchronous Ethernet on that port.

De-provisioning of the card or MDA containing the specified port is not permitted while the port is configured within PTP.

Changing the encapsulation or the port type of the Ethernet port is not permitted when PTP Ethernet Multicast operation is configured on the port.

Default N/A

Parameters *port-id* — specifies a specific physical port

Values *slot/mda/port*
 esat-id/slot/port
 pxc-id.sub-port

create — This keyword is required when first creating the PTP port, if the system is configured to require it (enabled in the environment create command). Once the PTP port is created, it is possible to navigate into the context without the create keyword.

address

Syntax **address** {01:1b:19:00:00:00|01:80:c2:00:00:0e}
 no address

Context config>port>ethernet>ptp>port

Description This command allows for the specification of the mac-address to be used for the destination MAC address of the transmitted ptp messages.

IEEE Std 1588-2008 Annex F defines two reserved addresses for 1588 messages. These are:

- **01-1B-19-00-00-00** — all except the peer delay mechanism messages
- **01-80-C2-00-00-0E** — peer delay mechanism messages

Both addresses are supported for reception independent of the address configured by this command.

The **no** form of this command sets the address to the default address.

Default address 01-1B-19-00-00-00

log-delay-interval

Syntax **log-delay-interval** *log-interval*

Context	config>system>ptp>port
Description	<p>This command configures the minimum interval used for multicast Delay_Req messages. This parameter is applied on a per port basis. For ports in a slave state, it shall be the interval used, unless the parent port indicates a longer interval. For a port in master state, it shall be the interval advertised to external slave ports as the minimum acceptable interval for Delay_Req messages from those slave ports.</p> <p>It is a requirement of the 1588 standard that a port in Slave state shall check the logMessageInterval field of received multicast Delay_Resp messages. If the value of the logMessageInterval field of those messages is greater than the value programmed locally for the generation of Delay_Req messages, then the Slave must change to use the greater value (i.e. longer interval) for the generation of Delay_Req messages. This requirement is supported in the router.</p> <p>The parameter is only applicable to ports and not to peers.</p>
Default	<p>log-delay-interval -6 for ieee1588-2008</p> <p>log-delay-interval -6 for g8265dot1-2010</p> <p>log-delay-interval -4 for g8275dot1-2014</p>
Parameters	<p><i>log-interval</i> — specifies the Delay_Req message interval, in log form</p> <p>Values [-6 to 0]</p>

log-sync-interval

Syntax	<p>log-sync-interval <i>log-interval</i></p> <p>no log-sync-interval</p>
Context	config>system>ptp>port
Description	<p>This command configures the message interval used for transmission of multicast Sync messages.</p> <p>For multicast messages used on PTP Ethernet ports, this configures the message interval used for Sync messages transmitted by the local node when the port is in Master state.</p>
Default	<p>log-sync-interval -6 (64 packets per second) for ieee1588-2008 or</p> <p>log-sync-interval -6 (64 packets per second) for g8265dot1-2010 or</p> <p>log-sync-interval -4 (16 packets per second) for g8275dot1-2014</p>
Parameters	<p><i>log-interval</i> — the message interval, in log form</p> <p>Values -6..0 This corresponds to a maximum rate of 64 packets per second, and a minimum rate of 1 packet per second.</p>

master-only

Syntax	master-only {true false}
Context	config>system>ptp>port
Description	This command is used to restrict the local port to never enter the slave state. Use the command to ensure that the 7750 SR never draws synchronization from the attached external device.

This parameter is only effective when the profile is set to g8275dot1-2014.



Note: The ITU-T G.8275.1 (07/2014) recommendation used the term 'notSlave' for this functionality; however, the IEEE has added this capability into the next edition of the 1588 standard using the term masterOnly. These are equivalent.

Default	master-only true
----------------	------------------

shutdown

Syntax	[no] shutdown
Context	config>system>ptp>port
Description	This command disables or enables a specific PTP port. When shutdown, all PTP Ethernet messages are dropped on the IOM They will not be counted in the PTP message statistics. No PTP packets are transmitted by the node toward this port.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last enabled port or peer cannot be shutdown. This prevents the user from having PTP enabled without any means to synchronize the local clock to a parent clock.

Default	no shutdown
----------------	-------------

priority1

Syntax	priority1 <i>priority</i> no priority1
Context	config>system>ptp
Description	This command configures the priority1 value of the local clock. This parameter is only used when the profile is set to ieee1588-2008. This value is used by the Best Master Clock Algorithm to determine which clock should provide timing for the network.

This value is used for the value to advertise in the Announce messages and for the local clock value in data set comparisons.

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

Default *priority1 128*

Parameters *priority* — specifies the value of the *priority1* field

Values 0 to 255

priority2

Syntax **priority2** *priority*
no priority2

Context config>system>ptp

Description This command configures the *priority2* value of the local clock. This parameter is only used when the profile is set to *ieee1588-2008* or *g8275dot1-2014*. The parameter is ignored when any other profile is selected.

This value is used by the Best Master Clock algorithm to determine which clock should provide timing for the network.



Note: This value is used for the value to advertise in the Announce messages and for local clock value in data set comparisons.

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

Default *priority2 128*

Parameters *priority* — specifies the value of the *priority2* field

Values 0 to 255

profile

Syntax **profile** {*g8265dot1-2010* | *ieee1588-2008* | *g8275dot1-2014*}

Context config>system>ptp

Description This command configures the profile to be used for the internal PTP clock. It defines the Best Master Clock Algorithm (BMCA) behavior.

The profile cannot be changed unless PTP is shutdown.

When you change the profile, the domain changes to the default value for the new profile. The **clock-type** is restricted based on the profile. If the profile is `ieee1588-2008` then the clock-type is not restricted. If the profile is `g8265dot1-2010` then the clock type may only be ordinary slave or ordinary master; boundary clock is not allowed. If the profile is `g8275dot1-2014` then the clock type may only be boundary clock; ordinary slave and ordinary master is not allowed.

When you change the profile, if any of the command parameters are set to default for the original profile, then the parameter will be changed to the default for the new profile. This applies to the following:

- **log-anno-interval** set for the clock
- **log-sync-interval** set for a peer or a port
- **log-delay-interval** set for a port

If the parameter is set to a value other than the default for the original profile, then its value will remain unchanged

Default	profile g8265dot1-2010
Parameters	g8265dot1-2010 — conform to the ITU-T G.8265.1 specification ieee1588-2008 — conform to the 2008 version of the IEEE1588 standard g8275dot1-2014 — conform to the ITU-T G.8275.1 specification

shutdown

Syntax	[no] shutdown
Context	config>system>ptp
Description	<p>This command disables or enables the PTP protocol. If PTP is disabled, the router will not transmit any PTP packets, and will ignore all received PTP packets. If the user attempts execute a no shutdown command on hardware that does not support PTP, an alarm will be raised to indicate limited capabilities.</p> <p>When PTP is shutdown, the PTP slave port is not operational. It shall not be considered as a source for system timing.</p> <p>On assemblies supporting a 1 PPS output interface, this command controls the presentation of a signal on that interface. When PTP is enabled, the 1 PPS port is enabled, and it generates a pulse whose rising edge represented the second rollover of the internal PTP time scale (that is, whenever the fractional second of the time is exactly zero). When PTP is disabled, no signal is presented on the 1 PPS interface.</p>
Default	shutdown

5.22.2.8 Date and Time Commands

set-time

Syntax	set-time [<i>date</i>] [<i>time</i>]
Context	admin
Description	<p>This command sets the local system time.</p> <p>The time entered should be accurate for the time zone configured for the system. The system will convert 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.</p> <p>If SNTP or NTP is enabled (no shutdown) then this command cannot be used.</p>
Default	N/A
Parameters	<p><i>date</i> — the local date and time accurate to the minute in the YYYY/MM/DD format</p> <p>Values <i>YYYY</i> is the four-digit year <i>MM</i> is the two-digit month <i>DD</i> is the two-digit date</p> <p><i>time</i> — the time (accurate to the second) in the <i>hh:mm[:ss]</i> format. If no seconds value is entered, the seconds are reset to :00.</p> <p>Values <i>hh</i> is the two-digit hour in 24 hour format (00=midnight, 12=noon) <i>mm</i> is the two-digit minute</p> <p>Default 0</p>

time

Syntax	time
Context	config>system
Description	This command enables the context to configure the system time zone and time synchronization parameters.
Default	N/A

5.22.2.9 Network Time Protocol Commands

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. Use the no form of the command to stop the execution of NTP and remove its configuration.
Default	N/A

authentication-check

Syntax	[no] authentication-check
Context	config>system>time>ntp
Description	<p>This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key 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.</p> <p>When authentication-check is enabled, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for type and one for key-id, one for type, value mismatches. These counters are visible in a show command.</p> <p>The no form of this command allows authentication mismatches to be accepted; the counters however are maintained.</p>
Default	authentication-check — rejects authentication mismatches

authentication-key

Syntax	authentication-key <i>key-id</i> key <i>key</i> [hash hash2] type { des message-digest } no authentication-key <i>key-id</i>
Context	config>system>time>ntp
Description	This command sets the authentication key-id, type and key used to authenticate NTP PDUs sent to or received by other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, type and key value must match.

The **no** form of the command removes the authentication key.

Default	N/A
Parameters	<p><i>key-id</i> — configures the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets</p> <p>Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry.</p> <p>Recipients of the NTP packets must have the same authentication key-id, type, and key value in order to use the data transmitted by this node. This is an optional parameter.</p> <p>Values 1 to 255</p> <p>Default None</p> <p>key — The authentication key associated with the configured key-id, the value configured in this parameter is the actual value used by other network elements to authenticate the NTP packet.</p> <p>The key can be any combination of ASCII characters up to 32 characters in length for message-digest (md5) or 8 characters in length for des (length limits are unencrypted lengths). If spaces are used in the string, enclose the entire string in quotation marks (".").</p> <p>hash — specifies 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</p> <p>hash2 — specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable 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.</p> <p>type — determines if DES or message-digest authentication is used</p> <p>This is a required parameter; either DES or message-digest must be configured.</p> <p>Values</p> <p>des — specifies that DES authentication is used for this key. The des option is not permitted in FIPS-140-2 mode.</p> <p>message-digest — specifies that MD5 authentication in accordance with RFC 2104 is used for this key</p>

broadcast

Syntax	broadcast [router <i>router-name</i>] { interface <i>ip-int-name</i> } [key-id <i>key-id</i>] [version <i>version</i>] [ttl <i>ttl</i>] no broadcast [router <i>router-name</i>] { interface <i>ip-int-name</i> }
Context	config>system>time>ntp

Description	<p>This command configures the node to transmit NTP packets on a given interface. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended.</p> <p>The no form of this command removes the address from the configuration.</p>
Default	N/A
Parameters	<p><i>router-name</i> — specifies the router name used to transmit NTP packets. Base is the default. Select management to use the management port (Ethernet port on the CPM).</p> <p>Values Base, management</p> <p>Default Base</p> <p><i>ip-int-name</i> — specifies the local interface on which to transmit NTP broadcast packets. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>Values 32 character maximum</p> <p>key-id <i>key-id</i> — identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets to and from an NTP server and peers. If an NTP packet is received by this node both authentication key and authentication type must be valid otherwise the packet will be rejected and an event/trap generated.</p> <p>Values 1 to 255</p> <p>Default none</p> <p>version <i>version</i> — specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all versions will be accepted.</p> <p>Values 1 to 4</p> <p>Default 4</p> <p>tll <i>tll</i> — specifies the IP Time To Live (TTL) value</p> <p>Values 1 to 255</p> <p>Default none</p>

broadcastclient

Syntax	<p>broadcastclient [router <i>router-name</i>] [interface <i>ip-int-name</i>] [authenticate]</p> <p>no broadcastclient [router <i>router-name</i>] [interface <i>ip-int-name</i>]</p>
Context	config>system>time>ntp

Description	<p>When configuring NTP, the node can be configured to receive broadcast packets on a given subnet. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended. If broadcast is not configured then received NTP broadcast traffic will be ignored. Use the show command to view the state of the configuration.</p> <p>The no form of this command removes the address from the configuration.</p>
Default	N/A
Parameters	<p><i>router router-name</i> — specifies the router name used to receive NTP packets</p> <p>Values Base, management</p> <p>Default Base</p> <p><i>interface ip-int-name</i> — specifies the local interface on which to receive NTP broadcast packets. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>Values 32 character maximum</p> <p>authenticate — specifies whether or not to require authentication of NTP PDUs. When enabled, NTP PDUs are authenticated upon receipt.</p>

multicast

Syntax	multicast [version version] [key-id key-id] no multicast
Context	config>system>time>ntp
Description	<p>This command configures NTP the node to transmit multicast packets on the CPM/CCM MGMT port. Broadcast and multicast messages can easily be spoofed; authentication is strongly recommended.</p> <p>The no form of this command removes the multicast address from the configuration.</p>
Default	N/A
Parameters	<p>version version — specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all three versions are accepted.</p> <p>Values 2 to 4</p> <p>Default 4</p> <p>key-id key-id — specifies the configured authentication key and authentication type used by this version to transmit NTP packets. If this command is omitted from the configuration, packets are sent unencrypted.</p> <p>Values 1 to 255</p> <p>Default None</p>

multicastclient

Syntax	multicastclient [authenticate] no multicastclient
Context	config>system>time>ntp
Description	<p>This command configures the node to receive multicast NTP messages on the CPM MGMT port. If multicastclient is not configured, received NTP multicast traffic will be ignored. Use the show command to view the state of the configuration.</p> <p>The no construct of this message removes the multicast client for the specified interface from the configuration.</p>
Default	N/A
Parameters	authenticate — This optional parameter makes authentication a requirement. If authentication is required, the authentication key-id received must have been configured in the authentication-key command, and that key-id type and key value must also match.

ntp-server

Syntax	ntp-server [authenticate] no ntp-server
Context	config>system>time>ntp
Description	<p>This command configures the node to assume the role of an NTP server. Unless the server command is used, this node will function as an NTP client only and will not distribute the time to downstream network elements.</p>
Default	no ntp-server
Parameters	<p>authenticate — if specified, makes authentication a requirement. If authentication is required, the authentication key-id received in a message must have been configured in the authentication-key command, and that key-id type and key value must also match.</p> <p>The authentication key from the received messages will be used for the transmitted messages.</p>

peer

Syntax	peer {ip-address ipv6-address} [key-id key-id] [version version] [prefer] no peer ip-address
Context	config>system>time>ntp

Description	<p>Configuration of an NTP peer configures symmetric active mode for the configured peer. Although any system can be configured to peer with any other NTP node it is recommended to configure authentication and to configure known time servers as their peers.</p> <p>The no form of the command removes the configured peer.</p>
Default	N/A
Parameters	<p><i>ipv6-address</i> — configures the IPv6 address of the peer that requires a peering relationship to be set up. The <i>ipv6</i> is applicable to the 7750 SR and 7950 XRS only.</p> <p>Values <i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i> (eight 16-bit pieces) <i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>x</i>:<i>d</i>.<i>d</i>.<i>d</i>.<i>d</i> <i>x</i> [0 to FFFF]H <i>d</i> [0 to 255]D</p> <p>Default None</p> <p><i>ip-address</i> — configures the IP address of the peer that requires a peering relationship to be set up. This is a required parameter.</p> <p>Values any valid IP-address</p> <p>Default None</p> <p>key-id <i>key-id</i> — Successful authentication requires that both peers must have configured the same authentication key-id, type and key value.</p> <p>Specify the <i>key-id</i> that identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP peer. If an NTP packet is received by this node, the authentication key-id, type, and key value must be valid otherwise the packet will be rejected and an event/trap generated.</p> <p>Values 1 to 255</p> <p>Default None</p> <p>version <i>version</i> — specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all three nodes are accepted.</p> <p>Values 2 to 4</p> <p>Default 4</p> <p>prefer — When configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.</p>

server

Syntax	server { <i>ip address</i> <i>ipv6-address</i> ptp } [key-id <i>key-id</i>] [version <i>version</i>] [prefer] no server <i>ip address</i>
---------------	--

Context	config>system>time>ntp
Description	<p>This command is used when the node should operate in client mode with the ntp server specified in the address field of this command. The no construct of this command removes the server with the specified address from the configuration.</p> <p>If the internal PTP process is to be used as a source of time for System Time and OAM time then it must be specified as a server for NTP. If PTP is specified then the prefer parameter must also be specified. Once PTP has established a UTC traceable time from an external grandmaster then it shall always be the source for time into NTP even if PTP goes into time holdover. PTP applies only to the 7450 ESS and 7750 SR.</p> <p>Use of the internal PTP time source for NTP will promote the internal NTP server to stratum 1 level. This may impact the NTP network topology.</p>
Default	N/A
Parameters	<p><i>ipv6-address</i> — configures the IPv6 address of the node that acts as an NTP server to this network element</p> <p>Values x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D</p> <p>Default None</p> <p><i>ip-address</i> — configures the IP address of a node that acts as an NTP server to this network element. This is a required parameter.</p> <p>Values any valid IP address</p> <p>ntp — configures the internal PTP process as a time server into the NTP process. The prefer parameter is mandatory with this server option (applies only to the 7450 ESS and 7750 SR).</p> <p>key-id <i>key-id</i> — enters the key-id that identifies 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 value must be valid otherwise the packet will be rejected and an event/trap generated. This is an optional parameter.</p> <p>Values 1 to 255</p> <p>version <i>version</i> — configures the NTP version number that is expected by this node. This is an optional parameter</p> <p>Values 2 to 4</p> <p>Default 4</p> <p>prefer — When configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.</p>

5.22.2.9.1 SNTP Commands

sntp

Syntax	[no] sntp
Context	config>system>time
Description	<p>This command creates the context to edit the Simple Network Time Protocol (SNTP).</p> <p>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.</p> <p>The system clock is automatically adjusted at system initialization time or when the protocol first starts up.</p> <p>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.</p> <p>SNTP is created in an administratively enabled state (no shutdown).</p> <p>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.</p>
Default	no sntp

broadcast-client

Syntax	[no] broadcast-client
Context	config>system>time>sntp
Description	<p>This command enables listening to SNTP/NTP broadcast messages on interfaces with broadcast client enabled at global device level.</p> <p>When this global parameter is configured then the ntp-broadcast parameter must be configured on selected interfaces on which NTP broadcasts are transmitted.</p> <p>SNTP must be shutdown prior to changing either to or from broadcast mode.</p> <p>The no form of the command disables broadcast client mode.</p>
Default	no broadcast-client

server-address

Syntax	server-address <i>ip-address</i> [version <i>version-number</i>] [normal preferred] [interval <i>seconds</i>] no server-address <i>ip-address</i>
Context	config>system>time>sntp
Description	This command creates an SNTP server for unicast client mode.
Default	N/A
Parameters	<i>ip-address</i> — specifies the IP address of the SNTP server version <i>version-number</i> — 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 interval <i>seconds</i> — specifies the frequency at which this server is queried Values 64 to 1024 Default 64

5.22.2.9.2 System Time Commands

dst-zone

Syntax	[no] dst-zone [<i>std-zone-name</i> <i>non-std-zone-name</i>]
Context	config>system>time
Description	<p>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.</p> <p>When configured, the time is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.</p> <p>If the time zone configured is listed in Table 30, 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 30 or entered as optional parameters in this command.</p>

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 will return 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 none — 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 30](#). 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 created using the [zone](#)

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 start of summer time settings.

Default end first sunday january 00:00

Parameters *end-week* — specifies the starting week of the month when the summer time will end

Values first, second, third, fourth, last

Default first

end-day — specifies the starting day of the week when the summer time will end

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default sunday

end-month — the starting month of the year when the summer time will take 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 will end

Values 0 to 24
Default 0

minutes — specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time will end

Values 0 to 59
Default 0

offset

Syntax	offset <i>offset</i>
Context	config>system>time>dst-zone
Description	This command specifies the number of minutes that will be added to the time when summer time takes effect. The same number of minutes will be subtracted from the time when the summer time ends.
Default	offset 60
Parameters	<i>offset</i> — 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 { <i>start-week</i> } { <i>start-day</i> } { <i>start-month</i> } [<i>hours-minutes</i>]
Context	config>system>time>dst-zone
Description	This command configures start of summer time settings.
Default	start first sunday january 00:00
Parameters	<i>start-week</i> — specifies the starting week of the month when the summer time will take effect Values first, second, third, fourth, last Default first

start-day — specifies the starting day of the week when the summer time will take effect

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default sunday

start-month — the starting month of the year when the summer time will take 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 will take effect

Default 0

minutes — specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time will take effect

Default 0

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 SR-series router OS supports system-defined and user-defined time zones. The system-defined time zones are listed in [Table 30](#).

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 will be 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 30](#). 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. Note that some system-defined time zones have implicit summer time settings which causes the switchover to summer time to occur automatically; 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 4 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 UTC + 9.5 hours.

Values hours: -11 to 11
minutes: 0 to 59

Default hours: 0
minutes: 0

5.22.2.10 Cron Commands

cron

Syntax	cron
Context	config
Description	<p>This command creates the context to create scripts, script parameters and schedules which support the Service Assurance Agent (SAA) functions.</p> <p>CRON features are saved to the configuration file on both primary and backup control modules. If a control module switchover occurs, CRON events are restored when the new configuration is loaded. If a control module switchover occurs during the execution of a cron script, the failover behavior will be determined by the contents of the script.</p>

schedule

Syntax	[no] schedule <i>schedule-name</i> [owner <i>owner-name</i>]
Context	config>system>cron
Description	<p>This command configures the type of schedule to run, including one-time only (oneshot), periodic or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute and interval (seconds).</p> <p>The no form of the command removes the context from the configuration.</p>
Default	N/A
Parameters	<p><i>schedule-name</i> — name of the schedule</p> <p>owner <i>owner-name</i> — owner name of the schedule</p>

day-of-month

Syntax	day-of-month { <i>day-number</i> [<i>..day-number</i>] all }
	no day-of-month
Context	config>system>cron>sched
Description	<p>This command specifies which days of the month that the schedule will occur. Multiple days of the month can be specified. When multiple days are configured, each of them will cause the schedule to trigger. If a day-of-month is configured without configuring month, weekday, hour and minute, the event will not execute.</p> <p>Using the weekday command as well as the day-of-month command will cause the script to run twice. For example, consider that today is Monday January 1. If Tuesday January 5 is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).</p> <p>The no form of this command removes the specified day-of-month from the list.</p>
Default	no day-of-month
Parameters	<p><i>day-number</i> — The positive integers specify the day of the month counting from the first of the month. The negative integers specify the day of the month counting from the last day of the month. For example, configuring day-of-month -5, 5 in a month that has 31 days will specify the schedule to occur on the 27th and 5th of that month.</p> <p>Integer values must map to a valid day for the month in question. For example, February 30 is not a valid date.</p> <p>Values 1 to 31, -31 to -1 (maximum 62 day-numbers)</p> <p>all — specifies all days of the month</p>

count

Syntax	count <i>number</i> no count				
Context	config>system>cron>sched				
Description	This command configures the total number of times a CRON “interval” 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	<i>number</i> — the number of times the schedule is run <table> <tr> <td>Values</td><td>1 to 65535</td></tr> <tr> <td>Default</td><td>65535</td></tr> </table>	Values	1 to 65535	Default	65535
Values	1 to 65535				
Default	65535				

end-time

Syntax	end-time [<i>date</i> <i>day-name</i>] <i>time</i> no end-time						
Context	config>system>cron>sched						
Description	This command is used concurrently with type periodic or calendar . Using the type of periodic , end-time determines at which interval the schedule will end. Using the type of calendar , end-time determines on which date the schedule will end. When no end-time is specified, the schedule runs forever.						
Default	no end-time						
Parameters	<i>date</i> — specifies the date to schedule a command <table> <tr> <td>Values</td><td>YYYY:MM:DD in year:month:day number format</td></tr> </table> <i>day-name</i> — specifies the day of the week to schedule a command <table> <tr> <td>Values</td><td>sunday, monday, tuesday, wednesday, thursday, friday, saturday</td></tr> </table> <i>time</i> — specifies the time of day to schedule a command <table> <tr> <td>Values</td><td>hh:mm</td></tr> </table>	Values	YYYY:MM:DD in year:month:day number format	Values	sunday, monday, tuesday, wednesday, thursday, friday, saturday	Values	hh:mm
Values	YYYY:MM:DD in year:month:day number format						
Values	sunday, monday, tuesday, wednesday, thursday, friday, saturday						
Values	hh:mm						

hour

Syntax	hour {.. <i>hour-number</i> [.. <i>hour-number</i>] all } no hour
---------------	--

Context	config>system>cron>sched
Description	<p>This command specifies which hour to schedule a command. Multiple hours of the day can be specified. When multiple hours are configured, each of them will cause the schedule to trigger. Day-of-month or weekday must also be specified. All days of the month or weekdays can be specified. If an hour is configured without configuring month, weekday, day-of-month, and minute, the event will not execute.</p> <p>The no form of this command removes the specified hour from the configuration.</p>
Default	no hour
Parameters	<p><i>hour-number</i> — specifies the hour to schedule a command</p> <p>Values 0 to 23 (maximum 24 hour-numbers)</p> <p>all — specifies all hours</p>

interval

Syntax	interval <i>seconds</i> no interval
Context	config>system>cron>sched
Description	This command specifies the interval between runs of an event.
Default	no interval
Parameters	<p><i>seconds</i> — the interval, in seconds, between runs of an event</p> <p>Values 30 to 4,294,967,295</p>

minute

Syntax	minute { <i>minute-number</i> [<i>..minute-number</i>] all } no minute
Context	config>system>cron>sched
Description	<p>This command specifies the minute to schedule a command. Multiple minutes of the hour can be specified. When multiple minutes are configured, each of them will cause the schedule to occur. If a minute is configured, but no hour or day is configured, the event will not execute. If a minute is configured without configuring month, weekday, day-of-month, and hour, the event will not execute.</p> <p>The no form of this command removes the specified minute from the configuration.</p>
Parameters	<p><i>minute-number</i> — specifies the minute to schedule a command</p> <p>Values 0 to 59 (maximum 60 minute-numbers)</p>

all — specifies all minutes

month

Syntax	month { <i>month-number</i> [.. <i>month-number</i>] <i>month-name</i> [.. <i>month-name</i>] all } no month
Context	config>system>cron>sched
Description	<p>This command specifies the month when the event should be executed. Multiple months can be specified. When multiple months are configured, each of them will cause the schedule to trigger. If a month is configured without configuring weekday, day-of-month, hour and minute, the event will not execute.</p> <p>The no form of this command removes the specified month from the configuration.</p>
Default	no month
Parameters	<p>month-number — specifies a month number</p> <p>Values 1 to 12 (maximum 12 month-numbers)</p> <p>all — specifies all months</p> <p>month-name — specifies a month by name</p> <p>Values january, february, march, april, may, june, july, august, september, october, november, december (maximum 12 month names).</p>

type

Syntax	type { <i>schedule-type</i> }
Context	config>system>cron>sched
Description	This command specifies how the system should interpret the commands contained within the schedule node.
Default	type periodic
Parameters	<p><i>schedule-type</i> — specifies the type of schedule for the system to interpret the commands contained within the schedule node</p> <p>Values periodic — specifies a schedule which runs at a given interval. interval must be specified for this feature to run successfully.</p> <p>calendar — specifies a schedule which runs based on a calendar. weekday, month, day-of-month, hour and minute must be specified for this feature to run successfully.</p> <p>oneshot — specifies a schedule which runs one time only.</p>

As soon as the first event specified in these parameters takes place and the associated event occurs, the schedule enters a shutdown state. [month](#), [weekday](#), [day-of-month](#), [hour](#) and [minute](#) must be specified for this feature to run successfully.

Default periodic

weekday

Syntax	weekday { <i>weekday-number</i> [<i>..weekday-number</i>] <i>day-name</i> [<i>..day-name</i>] all }
	no weekday
Context	config>system>cron>sched
Description	<p>This command specifies which days of the week that the schedule will fire on. Multiple days of the week can be specified. When multiple days are configured, each of them will cause the schedule to occur. If a weekday is configured without configuring month, day-of-month, hour and minute, the event will not execute.</p> <p>Using the weekday command as well as the day-of month command will cause the script to run twice. For example, consider that today is Monday January 1. If Tuesday January 5 is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).</p> <p>The no form of this command removes the specified weekday from the configuration.</p>
Default	no weekday
Parameters	<p>day-number — specifies a weekday number</p> <p> Values 1 to 7 (maximum 7 week-day-numbers)</p> <p>day-name — specifies a day by name</p> <p> Values sunday, monday, tuesday, wednesday, thursday, friday, saturday (maximum 7 weekday names)</p> <p>all — specifies all days of the week.</p>

5.22.2.11 Script Control Commands

script-control

Syntax	script-control
Context	config>system
Description	This command enables the context to configure command script parameters.

Default N/A

script-policy

Syntax **script-policy** *policy-name* [**owner** *policy-owner*]

Context config>system>script-control
config>system>cron>schedule

Description This command is used to configure the CLI script policy.

Parameters *policy-name* — specifies the name of the policy. Can be up to 32 characters
owner *policy-owner* — specifies the name of the policy owner. Can be up to 32 characters
The owner is an arbitrary name and not necessarily a user name. Commands in the scripts are not authorized against the owner. The **configure system security cli-script authorization x cli-user** command determines the user context against which commands in the scripts are authorized.

Default “TiMOS CLI”

expire-time

Syntax **expire-time** {*seconds* | **forever**}

Context config>system>script-control>script-policy

Description This command is used to configure the maximum amount of time to keep the run history status entry from a script run.

Default expire-time 3600

Parameters *seconds* — specifies the time to keep the run history status entry, in seconds

Values 0 to 21474836

Default 3600

forever — keyword to keep the run history status entry indefinitely

lifetime

Syntax **lifetime** {*seconds* | **forever**}

Context config>system>script-control>script-policy

Description This command is used to configure the maximum amount of time that a script may run.

Default	lifetime 3600
Parameters	<i>seconds</i> — specifies the maximum amount of time that a script may run, in seconds
Values	0 to 21474836
Default	3600
	forever — keyword to allow a script to run indefinitely

max-completed

Syntax	max-completed unsigned
Context	config>system>script-control>script-policy
Description	This command is used to configure the maximum number of script run history status entries to keep.
Default	max-completed 1
Parameters	<i>unsigned</i> — specifies the maximum number of script run history status entries to keep
Values	1 to 255
Default	1

results

Syntax	results file-url no results
Context	config>system>script-control>script-policy
Description	<p>This command is used to specify the location where the system writes the output of an event script's execution.</p> <p>The no form of the command removes the file location from the configuration. Scripts will not execute if there is no result location defined.</p>
Default	no results
Parameters	<p><i>file-url</i> — specifies the location to send CLI output from script runs. The <i>file-url</i> is a location, directory, and filename prefix to which a data and timestamp suffix is added when the results files are created during a script run, as follows:</p> <p><i>file-url_YYYYMMDD-hhmmss.uuuuuu.out</i> where:YYYYMMDD — date hhmmss — hours, minutes, and seconds uuuuuu — microseconds (padded to 6 characters with leading zeros)</p> <p>Values <i>local-url</i> <i>remote-url</i></p>

local-url — [*cflash-id*]/ [*file-path*]
200 chars max, including *cflash-id*
directory length 99 characters max each
remote url — [{ftp:// | tftp://}login:password@remote-
location/][*file-path*]
255 characters max
directory length 99 characters max each
remote-location — [hostname | ipv4-address | ipv6-address]
ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x[-interface]
x:x:x:x:x.d.d.d[-interface]
x — [0 to FFFF]H
d — [0 to 255]D
interface — 32 characters max, for link local addresses
cflash-id — cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-
A:, cf3-B:

script

Syntax	script <i>script-name</i> [owner <i>script-owner</i>] no script
Context	config>system>script-control>script-policy config>system>script-control
Description	This command is used to configure a script to be run. The no form of the command removes the script.
Default	no script
Parameters	<i>script-name</i> — specifies the name of the script. Can be up to 32 characters. owner <i>script-owner</i> — specifies the name of the script owner. Can be up to 32 characters. The owner is an arbitrary name and not necessarily a user name. Commands in the scripts are not authorized against the owner. The configure system security cli-script authorization x cli-user command determines the user context against which commands in the scripts are authorized. Default "TiMOS CLI"

location

Syntax	location <i>file-url</i> no location
---------------	---

Context	config>system>script-control>script
Description	<p>This command is used to identify the location of a script to be scheduled.</p> <p>The no form of the command removes the location.</p>
Default	no location
Parameters	<p><i>file-url</i> — specifies the location to search for scripts</p> <p>Values <i>local-url</i> <i>remote-url</i></p> <p> <i>local-url</i> — [<i>cflash-id</i>/] [<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 characters max each</p> <p> <i>remote url</i> — [{ftp:// tftp://}<i>login:password@remote-</i> <i>location</i>/][<i>file-path</i>] 255 characters max directory length 99 characters max each</p> <p> <i>remote-location</i> — [<i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i>]</p> <p> <i>ipv4-address</i> — <i>a.b.c.d</i></p> <p> <i>ipv6-address</i> — <i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x.d.d.d.d[-interface]</i> <i>x</i> — [0 to FFFF]H <i>d</i> — [0 to 255]D <i>interface</i> — 32 characters max, for link local addresses</p> <p> <i>cflash-id</i> — cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3- A:, cf3-B:</p>

5.22.2.12 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	disabled

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.
Default	N/A

begin

Syntax	begin
Context	config>system>sync-if-timing
Description	This command is required in order to enter the mode to create or edit the system synchronous interface timing configuration.
Default	N/A

bits

Syntax	bits
Context	config>system>sync-if-timing
Description	<p>This command enables the context to configure parameters for the Building Integrated Timing Supply (BITS). The settings specified under this context apply to both the BITS input and BITS output ports and to both the bits1 and bits2 ports on the 7750 SR-c4.</p> <p>The bits command subtree is only available on the 7450 ESS-7, 7450 ESS-12, 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-c4, 7950 XRS-20, 7950 XRS-40, 7950 XRS-16c, 7750 SR-a4, 7750 SR-a8, 7750 SR-1e, 7750 SR-2e, and 7750 SR-3e.</p>
Default	disabled

input

Syntax	input
Context	config>system>sync-if-timing>bits
Description	This command provides a context to enable or disable the external BITS timing reference inputs to the central clock of the router. In redundant systems with BITS ports, there are two possible BITS-in interfaces, one for each CPM or CCM. In the 7750 SR-c4 system, there are two bits ports on the CFM. The two BITS-in interfaces are configured together, but they are displayed separately in the show command.
Default	shutdown

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 configures the Building Integrated Timing Source (BITS) timing reference. The no form of the command reverts to the default configuration.
Default	interface-type ds1 esf
Parameters	<p>ds1 esf — specifies Extended Super Frame (ESF). This is a framing type used on DS1 circuits that consists of 24 192-bit frames. The 193rd bit provides timing and other functions.</p> <p>ds1 sf — specifies Super Frame (SF), also called D4 framing. This 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.</p> <p>e1 pcm30crc — specifies the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with CRC protection.</p> <p>e1 pcm31crc — specifies the pulse code modulation (PCM) type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.</p> <p>2048khz-g703 — specifies the 2048 kHz synchronization interface (T12) of ITU-T G.703. This parameter is only available on the 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12 when there is a CPM5 or later installed. It is also available on the 7750 SR-12e, 7750 SR-a4, 7750 SR-a8, 7750 SR-1e, 7750 SR-2e, and 7750 SR-3e.</p>

output

Syntax	output
Context	config>system>sync-if-timing>bits
Description	This command provides a context to configure and enable or disable the external BITS timing reference output to the central clock of the router. On redundant systems, there are two possible BITS-out interfaces, one for each CPM or CCM. On the 7750 SR-c4 system, there are two possible BITS-out interfaces on the chassis front panel. The two BITS-out interfaces are configured together, but they are displayed separately in the show command.
Default	shutdown

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 parameter of the BITS output, This is the distance in feet between the network element and the office clock (BITS/SSU). There are two possible BITS-out interfaces, one for each CPM. They are configured together, but they are displayed separately in the show command. This command is only applicable when the interface-type is DS1.
Default	line-length 110
Parameters	<p>110 — distance is from 0 to 110 feet</p> <p>220 — distance is from 110 to 220 feet</p> <p>330 — distance is from 220 to 330 feet</p> <p>440 — distance is from 330 to 440 feet</p> <p>550 — distance is from 440 to 550 feet</p> <p>660 — distance is from 550 to 660 feet</p>

source

Syntax	source { line-ref internal-clock }
Context	config>system>sync-if-timing>bits>output
Description	This command configures the values used to identity the source of the BITS (Building Integrated Timing Supply) output. This is either the signal recovered directly from ref1, ref2 or ptp, or it is the output of the node's central clock. The directly recovered signal would be used when the BITS output signal is feeding into an external stand alone timing distribution device (BITS/SASE). The specific directly recovered signal used is the best of the available signals based of the QL and/or the ref-order. The central clock output would be used when no BITS/SASE device is present and the BITS output signal is used to monitor the quality of the recovered clock within the system.
Default	source line-ref
Parameters	<p>line-ref — specifies that the BITS output timing is selected from one of the input references, without any filtering</p> <p>internal-clock — specifies that the BITS output timing is driven from the system timing</p>

ssm-bit

Syntax	ssm-bit <i>sa-bit</i>
Context	<p>config>system>sync-if-timing>bits</p> <p>config>system>sync-if-timing>ref1 (7750 SR-c12 only)</p> <p>config>system>sync-if-timing>ref2 (7750 SR-c12 only)</p>

Description	This command configures which sa-bit to use for conveying SSM information when the interface-type is E1.
Default	ssm-bit 8
Parameters	<i>sa-bit</i> — specifies the sa-bit value
Values	4 to 8

commit

Syntax	commit
Context	config>system>sync-if-timing
Description	This command saves changes made to the system synchronous interface timing configuration.
Default	N/A

ref-order

Syntax	ref-order <i>first second [third [fourth]]</i> no ref-order
Context	config>system>sync-if-timing
Description	<p>The synchronous equipment timing subsystem can lock to different timing reference inputs, those specified in the ref1, ref2, bits and ptp (ptp applies only to the 7450 ESS and 7750 SR) command configuration. This command organizes the priority order of the timing references.</p> <p>If a reference source is disabled, then the clock from the next reference source as defined by ref-order is used. If all reference sources are disabled, then clocking is derived from a local oscillator.</p> <p>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.</p> <p>For 7450 ESS and 7750 SR systems with two SF/CPM modules, the system distinguishes between the BITS inputs on the active and standby CPMs. The active CPM will use its BITS input port providing that port is qualified. If the local port is not qualified, then the active CPM will use the BITS input port from the standby CPM as the next priority reference. For example, the normal ref-order of bits ref1 ref2 will actually be bits (active CPM), followed by bits (standby CPM), followed by ref1, followed by ref2.</p>

For 7750 SR-c4 systems, the system distinguishes between the two BITS inputs on the CFM. The CFM will use its BITS input port **bits1** providing that port is qualified. If port **bits1** is not qualified, then the CFM will use the BITS input port **bits2** as the next priority reference. For example, the normal ref-order of **bits ref1 ref2** will actually be **bits1** followed by **bits2**, followed by **ref1**, followed by **ref2**.

For 7950 XRS systems with two SF/CPMs and two CCMs, the system distinguishes between the BITS inputs on the CCMs associated with the active and standby CPMs. The active CPM will use the BITS input port on the associated CCM, provided that the port is qualified. If the local port is not qualified, then the active CPM will use the BITS input port from the CCM associated with the standby CPM as the next priority reference. For example, the normal ref-order of **bits ref1 ref2** will actually be **bits** (active CCM), followed by **bits** (standby CCM), followed by **ref1**, followed by **ref2**.

The **no** form of the command resets the reference order to the default values.

The **bits** option is not supported on the 7750 SR-c12 chassis.

Default **bits ref1 ref2 ptp** (7750 SR and 7450 ESS)

bits ref1 ref2 (7950 XRS)

Parameters *first* — specifies the first timing reference to use in the reference order sequence

Values **ref1, ref2, bits, ptp**

second — specifies the second timing reference to use in the reference order sequence

Values **ref1, ref2, bits, ptp**

third — specifies the third timing reference to use in the reference order sequence

Values **ref1, ref2, bits, ptp**

ptp

Syntax **ptp**

Context config>system>sync-if-timing

Description	This command enables the context to configure parameters for system timing via IEEE 1588-2008, Precision Time Protocol. This command only applies to the 7450 ESS-7, 7450 ESS-12, and all 7750 SRs except for the 7750 SR-1e, 7750 SR-2e, and 7750 SR-3e.
--------------------	---

Default shutdown

ql-override

Syntax **ql-override** {**prs** | **stu** | **st2** | **tnc** | **st3e** | **st3** | **eec1** | **sec** | **prc** | **ssu-a** | **ssu-b** | **eec2**}

Context	config>system>sync-if-timing>bits config>system>sync-if-timing>ptp config>system>sync-if-timing>ref1 (7750 SR-c12 only) config>system>sync-if-timing>ref2 (7750 SR-c12 only)
Description	This command configures the QL value to be used for the reference for SETS input selection and BITS output. This value overrides any value received by that reference's SSM process.
Default	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 eec1 — Ethernet Equipment Clock Option 1 Traceable (sdh) eec2 — Ethernet Equipment Clock Option 2 Traceable (sonet) 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

ql-selection

Syntax	[no] ql-selection
Context	config>system>sync-if-timing
Description	When enabled the selection of system timing reference and BITS output timing reference takes into account quality level. Quality level is conveyed via the SSM or forced using the ql-override command.
Default	no ql-selection

ref1

Syntax	ref1
Context	config>system>sync-if-timing
Description	This command enables the context to configure parameters for the first timing reference.

The restrictions on the location for the source-port or source-bits for **ref1** and **ref2** are listed in [Table 44](#).

Table 44 Ref1 and Ref2 Timing References

Platform	Ref1 Slots	Ref2 Slots	Notes
7450 ESS-6/6v	1 to 2	3 to 4	—
7450 ESS-7	1 to 2	3 to 5	—
7450 ESS-12	1 to 5	6 to 10	—
7750 SR-1e	1	1	Ref1 and ref2 cannot be on the same MDA
7750 SR-2e	1 to 2	1 to 2	Ref1 and ref2 cannot be on the same MDA
7750 SR-3e	1 to 3	1 to 3	Ref1 and ref2 cannot be on the same MDA
7750 SR-7	1 to 2	3 to 5	—
7750 SR-12	1 to 5	6 to 10	—
7750 SR-12e	1 to 5	6 to 10	—
7750 SR-a4	1	1	—
7750 SR-a8	1 to 2	1 to 2	Ref1 and ref2 cannot be on the same slot
7750 SR-c4	1	1	Ref1 and ref2 cannot be on the same MDA/CMA
7750 SR-c12	1	1	Ref1 and ref2 cannot be on the same MDA/CMA
7950 XRS-16c	1 to 8	1 to 8	Ref1 and ref2 cannot be on the same slot
7950 XRS-20	1 to 10	1 to 10	Ref1 and ref2 cannot be on the same slot
7950 XRS-40	1 to 10	1 to 10	Ref1 and ref2 cannot be on the same slot

Default N/A

bits-interface-type

Syntax	bits-interface-type { ds1 [{ esf sf }] e1 [{ pcm30crc pcm31crc }] no bits-interface-type
Context	config>system>sync-if-timing>ref1 config>system>sync-if-timing>ref2
Description	This command configures the interface type of the BITS timing reference. The no form of the command reverts to the default configuration
Default	bits-interface-type ds1 esf
Parameters	<p>ds1 esf — specifies Extended Super Frame (ESF). This is a framing type used on DS1 circuits that consists of 24 192-bit frames. The 193rd bit provides timing and other functions.</p> <p>ds1 sf — specifies Super Frame (SF), also called D4 framing. This 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.</p> <p>e1 pcm30crc — specifies the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with CRC protection.</p> <p>e1 pcm31crc — specifies the pulse code modulation (PCM) type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.</p>

source-bits

Syntax	source-bits <i>slot/mda</i> no source-bits
Context	config>system>sync-if-timing>ref1 config>system>sync-if-timing>ref2
Description	This command configures the source bits for ref1 or ref2 timing reference. There are restrictions on the source-bits location for ref1 and ref2 based on platform. Refer to the description of the ref1 command for details. This command is only applicable to the 7750 SR-c12 chassis.
Default	N/A
Parameters	<p><i>slot/mda</i> — specifies the chassis slot and MDA containing the BITS port to be used as one of the two timing reference sources in the system timing subsystem</p> <p>Values slot:1 mda:1 to 12</p>

source-port

Syntax	source-port <i>port-id</i> no source-port
Context	config>system>sync-if-timing>ref1 config>system>sync-if-timing>ref2
Description	<p>This command configures the source port for timing reference ref1 or ref2. If the port is unavailable or the link is down, then the reference sources are re-evaluated according to the reference order configured in the ref-order command.</p> <p>In addition to physical port on the 7750 SR, T1 or E1 channels on a Channelized OC3/OC12/STM1/STM4 Circuit Emulation Service port can be specified if they are using adaptive timing.</p> <p>There are restrictions on the source-port location for ref1 and ref2 based on platform. Refer to the description of the ref1 command for details.</p>
Default	no source-port
Parameters	<i>port-id</i> — identifies the physical port in the <i>slot/mda/port</i> , <i>esat-id/slot/port</i> , or <i>pxc-id.sub-port</i> format

ref2

Syntax	ref2
Context	config>system>sync-if-timing
Description	<p>This command enables the context to configure parameters for the second timing reference. There are restrictions on the source-port and source-bits locations for ref2 based on the platform. The restrictions on the location for the source-port or source-bits for ref1 and ref2 are listed in Table 42.</p>
Default	N/A

revert

Syntax	[no] revert
Context	config>system>sync-if-timing
Description	<p>This command allows the clock to revert to a higher priority reference if the current reference goes offline or becomes unstable. When the failed reference becomes operational, it is eligible for selection. When the mode is non-revertive, a failed clock source is not selected again.</p>
Default	no revert

5.22.2.13 System Administration Commands

admin

Syntax	admin
Context	<root>
Description	The context to configure administrative system commands. Only authorized users can execute the commands in the admin context.
Default	N/A

application-assurance

Syntax	application-assurance
Context	admin
Description	This command enables the context to perform application-assurance operations.
Default	N/A

upgrade

Syntax	upgrade
Context	admin>app-assure
Description	This command loads a new protocol list from the isa-aa.tim file into the CPM. This command requires an ISA-AA reboot.
Default	N/A

clear-policy-lock

Syntax	clear-policy-lock
Context	admin
Description	This command allows an authorized administrator to clear an exclusive policy lock. This will reset the lock flag and end the policy editing session in progress, aborting any policy edits.
Default	N/A

debug-save

Syntax	debug-save [<i>file-url</i>]
Context	admin
Description	This command saves existing debug configuration (configuration done under the debug branch of CLI). Debug configurations are not saved by the admin save command and not preserved across a node reboot. The debug-save command makes the debug configuration available for the operator to execute after a reboot by using the exec command, if desired.
Default	N/A
Parameters	<i>file-url</i> — the file URL location to save the debug configuration. If no file-url is specified then the debug configuration is saved at the same location as the standard configuration file (bof>primary-image/bof>secondary-image/bof>tertiary-image) with the same file name as the standard configuration file but with a .dbg suffix.



Note: Ipv6-address applies only to the 7750 SR and 7950 XRS.

Values

file url	local-url remote-url: 255 chars max
local-url	[<i>cflash-id</i>][<i>file-path</i>] 200 chars max, including cflash-id directory length 99 chars max each
remote-url	[ftp://login:pswd@remote-locn/][<i>file-path</i>] 247 chars max directory length 99 chars max each
<i>remote-locn</i>	[hostname ipv4-address [ipv6-address]]
<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D interface - 32 chars max, for link local addresses 255
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

disconnect

Syntax	disconnect [address <i>ip-address</i> username <i>user-name</i> console telnet ftp ssh netconf]
---------------	---

Context	admin
Description	<p>This command disconnects a user from a session.</p> <p>Disconnect without any parameters will disconnect the session in which the command was executed.</p> <p>If any of the session type options (for example, console, telnet, FTP, SSH) are specified, then only the respective sessions are affected.</p> <p>If no session type options are specified, then all sessions from the IP address or from the specified user are disconnected.</p> <p>Any task that the user is executing is terminated. FTP files accessed by the user will not be removed.</p> <p>A major severity security log event is created specifying what was terminated and by whom.</p>
Default	none — no disconnect options are configured
Parameters	address <i>ip-address</i> — the IP address to disconnect, specified in dotted decimal notation



Note: Ipv6 is supported on the 7750 SR and 7950 XRS.

Values

<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D

- username** *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 session
- netconf** — disconnects the NETCONF session

display-config

Syntax **display-config** [**detail** | **index**]

Context	admin
Description	<p>This command displays the system's running configuration.</p> <p>By default, only non-default settings are displayed.</p> <p>Specifying the detail option displays all default and non-default configuration parameters.</p>
Default	N/A
Parameters	<p>detail — displays default and non-default configuration parameters</p> <p>index — displays only persistent-indices</p>

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).

Default	N/A
----------------	-----

oes

Syntax	oes
Context	admin
Description	This command creates or edits the context to run administrative commands on the Optical Extension Shelf (OES) subsystem.



Note: OES is only supported on the 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7950 XRS-20, and 7950 XRS-40 routers.

Default	Disabled
----------------	----------

force-switchover

Syntax	force-switchover <i>chassis-id</i> [now]
Context	admin>oes
Description	This command forces a switchover of the EC cards in the specified OES chassis. If the two EC cards are not synchronized, this command will return an error. If the now keyword is used, a switchover will occur even if the EC cards are not synchronized.
Default	N/A
Parameters	<i>chassis-id</i> — specifies the OES chassis ID
Values	oes-1

reboot

Syntax	reboot [now]
Context	admin>oes
Description	This command forces a cold reboot of the EC cards in the OES subsystem. This operation affects service.
Default	N/A

radius-discovery

Syntax	radius-discovery
Context	admin
Description	This command performs RADIUS discovery operations.
Default	N/A

force-discover

Syntax	force-discover [svc-id <i>service-id</i>]
Context	admin>radius-discovery
Description	When enabled, the server is immediately contacted to attempt discovery.
Default	N/A

Parameters	svc-id <i>service-id</i> — specifies an existing service ID
Values	1 to 2147483648 <i>svc-name</i> , up to 64 char max

reboot

Syntax	reboot [active standby upgrade] [hold] [now]
Context	admin
Description	<p>This command reboots the router or one CPM and can also be used to force an upgrade of the system boot ROMs.</p> <p>If no options are specified, the user is prompted to confirm the reboot operation. Answering yes (y) will result in both CPMs and all IOMs rebooting.</p> <pre>ALA-1>admin# reboot Are you sure you want to reboot (y/n)?</pre>
Default	N/A
Parameters	<p>active — keyword to reboot the active CPM</p> <p>Default active</p> <p>standby — keyword to reboot the standby CPM</p> <p>Default active</p> <p>upgrade — forces card firmware to be upgraded during chassis reboot. Normally, the SR-series router OS automatically performs firmware upgrades on CPMs and XCM/IOM cards without the need for the upgrade keyword. The automatic upgrade must be enabled in the SR OS7 Command Line Interface (CLI) when rebooting the system.</p> <p>When the upgrade keyword is specified, a chassis flag is set for the BOOT Loader (boot.ldr) and on the subsequent boot of the OS on the chassis, firmware images on CPMs, XCMs, or IOMs will be upgraded automatically.</p> <p>Any CPMs, XCMs, or IOMs 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.</p> <p>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.</p> <p>During any firmware upgrade, automatic or manual, it is imperative that during the upgrade procedure:</p> <ul style="list-style-type: none">• 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. The progress of a firmware upgrade can be monitored at the console.

hold — administratively hold a rebooted standby SF/CPM from coming back online. Both the control processor (CPM) and the switch fabric (SFM) of the standby SF/CPM are held out of service. This may be useful for troubleshooting purposes (e.g. standby SF/CPM is suspected of causing some system problems). The SF/CPM should not be left offline as the system does not have control or switch fabric redundancy while one SF/CPM is offline. The SF/CPM must be rebooted again (without the **hold** keyword) to return it to service. This parameter applies only to the SF/CPM3 and SF/CPM4 on the 7450 ESS and 7750 SR platforms. Note that on platforms such as the 7750 SR-12e and 7950 XRS, and on the 7450/7750 SFM5/CPM5, the SFMs are modeled as separate entities and can be administratively disabled by using the **configure sfm x shutdown** command.

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:

```
A:ALA-1>admin# save ftp://test:test@192.168.x.xx/./100.cfg
Saving configuration .....Completed.
```

An **admin save** operation initiated by a user is aborted if another user initiates another **admin save** from another session.

By default, the running configuration is saved to the primary configuration file.

Default N/A

Parameters *file-url* — the file URL location to save the configuration file

Values

<i>local-url remote-url</i>	
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>][<i>file-path</i>] 247 chars max directory length 99 chars max each
<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> "[" <i>ipv6-address</i> "]"]
<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D interface - 32 chars max, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Default the primary configuration file location

detail — saves both default and 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 indices.

satellite

Syntax	satellite [eth-sat <i>sat-id</i>] [reboot] [upgrade] [now] satellite [eth-sat <i>sat-id</i>] [sync-boot-env] satellite [eth-sat <i>sat-id</i>] [tech-support <i>file-url</i>]
Context	admin
Description	<p>This command can be used to perform administrative functions on the specified Ethernet-satellite chassis.</p> <p>If the reboot keyword is specified, the command initiates an administrative reboot of the specified Ethernet-satellite chassis.</p> <p>If the sync-boot-env keyword is specified, the command forces the specified Ethernet-satellite chassis to synchronize the boot image.</p> <p>If the tech-support keyword is specified, the command creates a system core dump. If the <i>file-url</i> parameter is omitted and a ts-location is defined, the SR OS automatically generates a file name for the tech-support file based on the system name, date and time. The file is saved to the directory indicated by the configured ts-location. See the command description of ts-location on page 457 for more information.</p>

The format of the auto-generated filename is ts-XXXXX.YYYYMMDD.HHMMUTC.dat where:

- XXXXX: system name with special characters expanded to avoid problems with file systems (for example, a '.' is expanded to %2E.)
- YYYYMMDD: Date with leading zeros on year, month and day
- HHMM: Hours and Minutes in UTC time (24hr format, always 4 chars, with leading zeros on hours and minutes)



Note: The **satellite** [**eth-sat** *sat-id*] [**tech-support** *file-url*] command should only be used with authorized direction from the Nokia Technical Assistance Center (TAC).

Default N/A

Parameters **eth-sat** *sat-id* — specifies the Ethernet-satellite chassis
file-url — specifies the file URL location to save the configuration file

Values

local-url | *remote-url*
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]
247 chars max
directory length 99 chars max each

now — keyword causes the satellite to reboot immediately without further prompts or interactive confirmation

reboot — keyword initiates a satellite reboot

sync-boot-env — keyword causes the specified Ethernet-satellite chassis to synchronize the boot image

upgrade — keyword causes the satellite to update its firmware image during chassis reboot

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* is defined, then the **tech support** file will have an automatic SR OS generated file name based on the system name and the date and time and 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: system name with special characters expanded to avoid problems with file systems (for example, a '.' is expanded to %2E.)
- YYYYMMDD: Date with leading zeros on year, month and day
- HHMM: Hours and Minutes in UTC time (24hr format, always 4 chars, with leading zeros on hours and minutes)



Note: This command should only be used with authorized direction from the Nokia Technical Assistance Center (TAC).

Default	N/A
Parameters	<i>file-url</i> — the file URL location to save the binary file
	Values
	<i>local-url</i> <i>remote-url</i>
<i>local-url</i>	[<i>cflash-id</i>]/[<i>file-path</i>] 200 chars max, including <i>cflash-id</i> directory length 99 chars max each
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>]/[<i>file-path</i>] 247 chars max directory length 99 chars max each
<i>remote-locn</i>	[<i>hostname</i> <i>ipv4-address</i> "[" <i>ipv6-address</i> "]"]
<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D interface - 32 chars max, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

ts-location

Syntax	ts-location <i>file-url</i> no ts-location
Context	config>system>security
Description	The ts-location command is used (along with an automatic system generated file name) when no <i>file-url</i> parameter is provided for the admin tech-support command. If no ts-location is defined then the operator must provide a file-url with the admin tech-support command itself.

The directory specified for the ts-location is not auto-created by SR OS. The operator must ensure that it exists.

Please see the **admin tech-support** command for more details about the system generated file name.

Default no ts-location

Parameters *file-url* — specifies the destination directory for auto-named tech-support files (when no *file-url* is specified with the 'admin tech-support' command). The *file-url* for the **ts-location** must be a directory (no filename or extension). The root directory (for example, cf1:\) is blocked for local compact flash destinations. A sub-directory (for example, cf2:\tech-support) must be used if local cf is the location.

Values

<i>local-url remote-url</i>	
<i>local-url</i>	[<i>cflash-id</i>][<i>file-path</i>] 200 chars max, including cflash-id directory length 99 chars max each
<i>remote-url</i>	[ftp:// <i>login:pswd@remote-locn</i>][<i>file-path</i>] 247 chars max directory length 99 chars max each
<i>remote-locn</i>	[<i>hostname ipv4-address "["ipv6-address"]"]</i>
<i>ipv4-address</i>	<i>a.b.c.d</i>
<i>ipv6-address</i>	<i>x:x:x:x:x:x:x[-interface]</i> <i>x:x:x:x:x:x:d.d.d.d[-interface]</i> <i>x</i> - [0 to FFFF]H <i>d</i> - [0 to 255]D interface - 32 chars max, for link local addresses
<i>cflash-id</i>	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

view

Syntax	view { bootup-cfg active-cfg candidate-cfg latest-rb <i>checkpoint-id</i> rescue }
Context	<root>
Description	The context to configure administrative system viewing parameters. Only authorized users can execute the commands in the admin context.
Default	N/A
Parameters	bootup-cfg — specifies the bootup configuration active-cfg — specifies current running configuration candidate-cfg — specifies candidate configuration

- latest-rb** — specifies the latest configuration
- checkpoint-id* — specifies a specific checkpoint file configuration
 - Values** 1 to 9
- rescue** — specifies a rescue checkpoint configuration

5.22.2.14 Redundancy Commands

redundancy

Syntax	redundancy
Context	admin config
Description	This command enters the context to allow the user to perform redundancy operations.
Default	N/A

force-switchover

Syntax	force-switchover [now] [ignore-status]
Context	admin>redundancy
Description	This command forces a switchover to the standby CPM card. The primary CPM reloads its software image and becomes the secondary CPM.
Default	N/A
Parameters	now — forces the switchover to the redundant CPM card immediately ignore-status — forces a switchover despite any diagnostics or conditions on the standby. For the 7950 XRS, this is true even if the standby cannot reach the extension CPMs on the extension chassis of an XRS-40 via its local CPM interconnect ports).

rollback-sync

Syntax	rollback-sync
Context	admin>redundancy

Description	This command copies the entire set of rollback checkpoint files from the active CPM CF to the inactive CPM CF.
--------------------	--

Default	N/A
----------------	-----

synchronize

Syntax	synchronize {boot-env config} no synchronize
---------------	---

Context	admin>redundancy
----------------	------------------

Description	This command performs a synchronization of the standby CPM's images and/or configuration files to the active CPM. Either the boot-env or config parameter must be specified.
--------------------	--

In the **admin>redundancy** context, this command performs a manually triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPM have identical operational parameters. This includes the saved configuration, CPM, XCM, and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM. 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).

The **no** form of the command removes the parameter from the configuration.

Default	no synchronize
----------------	----------------

Parameters	boot-env — synchronizes all files required for the boot process (loader, BOF, images, and config) config — synchronizes only the primary, secondary, and tertiary configuration files
-------------------	--

mgmt-ethernet

Syntax	mgmt-ethernet [revert seconds] no mgmt-ethernet
---------------	--

Context	config>redundancy
----------------	-------------------

Description	<p>If the management Ethernet port on the active CPM goes down, this command allows the active CPM to be configured to use the management Ethernet port of the standby CPM.</p> <p>The revert option allows the administrator to control when to revert back to the management Ethernet port of the primary CPM once it comes up again.</p> <p>The no form of the command disables redundancy, so that connectivity to the active CPM is lost if its Ethernet port goes down.</p> <p>This feature is not supported on the 7750 SR-a, 7750 SR-c, 7750-e, and the VSR platforms.</p>
Default	mgmt-ethernet 5 seconds
Parameters	<p><i>seconds</i> — specifies the duration to wait (in seconds) before reverting back to the primary CPM's management Ethernet port</p> <p>Values 1 to 300</p>

multi-chassis

Syntax	multi-chassis
Context	config>redundancy
Description	This command enables the context to configure multi-chassis parameters.
Default	N/A

bgp-multi-homing

Syntax	bgp-multi-homing
Context	config>redundancy
Description	This command configures BGP multi-homing parameters.
Default	N/A

site-min-down-timer

Syntax	site-min-down-timer <i>min-down-time</i> no site-min-down-timer
Context	config>redundancy>bgp-multi-homing

Description This command configures the BGP multi-homing site minimum down time. When set to a non-zero value, if the site goes operationally down it will remain operationally down for at least the length of time configured for the **site-min-down-timer**, regardless of whether other state changes would have caused it to go operationally up. This timer is restarted every time that the site transitions from up to down.

The above operation is optimized in the following circumstances:

- If the site goes down on the designated forwarder but there are no BGP multi-homing peers with the same site in an UP state, then the **site-min-down-timer** is not started and is not used.
- If the site goes down on the designated forwarder but there are no active BGP multi-homing peers, then the **site-min-down-timer** is not started and is not used.
- If the **site-min-down-timer** is active and a BGP multi-homing update is received from the designated forwarder indicating its site has gone down, the **site-min-down-timer** is immediately terminated and this PE becomes the designated forwarder if the BGP multi-homing algorithm determines it should be the designated forwarder.

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

Default no site-min-down-timer

Parameters *min-down-time* — specifies the time, in seconds, that a BGP multi-homing site remains operationally down after a transition from up to down

Values 1 to 100 seconds

Default 0 seconds

boot-timer

Syntax **boot-timer** *seconds*
no boot-timer

Context config>redundancy>bgp-multi-homing

Description This command configures the time the service manger waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.

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

Default no boot-timer

Parameters *seconds* — specifies the BGP multi-homing boot-timer in seconds

Values 1 to 100

site-activation-timer

Syntax	site-activation-timer <i>seconds</i> no site-activation-timer				
Context	config>redundancy>bgp-multi-homing				
Description	<p>This command defines the amount of time the service manager will keep the local sites in standby status, waiting for BGP updates from remote PEs before running the DF election algorithm to decide whether the site should be unblocked. The timer is started when one of the following events occurs if the site is operationally up:</p> <ul style="list-style-type: none"> • Manual site activation using the no shutdown command at site-id level or at member object(s) level (SAP(s) or PW(s)) • Site activation after a failure 				
Default	no site-activation-timer				
Parameters	<i>seconds</i> — specifies the standby status in seconds				
	<table> <tr> <td>Values</td><td>1 to 100</td></tr> <tr> <td>Default</td><td>2</td></tr> </table>	Values	1 to 100	Default	2
Values	1 to 100				
Default	2				

cert-sync

Syntax	[no] cert-sync
Context	admin>redundancy
Description	This command automatically synchronizes the certificate/CRL/key when importing or generating (for the key). Also if a new CF card is inserted into slot3 into the backup CPM, the system will sync the whole system-pki directory from the active CPM.
Default	enabled

rollback-sync

Syntax	[no] rollback-sync
Context	config>redundancy
Description	<p>The operator can enable automatic synchronization of rollback checkpoint files between the active CPM and inactive CPM. When this automatic synchronization is enabled, a rollback save will cause the new checkpoint file to be saved on both the active and standby CPMs. The suffixes of the old checkpoint files on both active and standby CPMs are incremented. Note that automatic sync only causes the ONE new checkpoint file to be copied to both CFs (the other 9 checkpoints are not automatically copied from active to standby but that can be done manually with admin red rollback-sync).</p>

Automatic synchronization of rollback checkpoint files across CPMs is only performed if the rollback-location is configured as a local file-url (for example, "cf3:/rollback-files/rollback). Synchronization is not done if the rollback-location is remote.

The **config red sync {boot-env | config}** and **admin red sync {boot-env | config}** do not apply to rollback checkpoint files. These commands do not manually or automatically sync rollback checkpoint files. The dedicated **rollback-sync** commands must be used to sync rollback checkpoint files.

Default no rollback-sync

synchronize

Syntax **synchronize {boot-env | config}**

Context config>redundancy

Description This command performs a synchronization of the standby CPMs images and/or config files to the active CPM. Either the **boot-env** or **config** parameter must be specified. In the **config>redundancy** context, this command performs an automatically triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPMs have identical operational parameters. This includes the saved configuration, CPM, XCM, and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM.

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 enabled

Parameters **boot-env** — synchronizes all files required for the boot process (loader, BOF, images, and config)
config — synchronize only the primary, secondary, and tertiary configuration files
Default **config**

5.22.2.14.1 Peer Commands

peer

Syntax	[no] peer <i>ip-address</i>
Context	config>redundancy>multi-chassis
Description	This command configures a multi-chassis redundancy peer.
Default	N/A
Parameters	<i>ip-address</i> — specifies a peer IP address. Multicast addresses are not allowed

authentication-key

Syntax	authentication-key [<i>authentication-key</i> <i>hash-key</i>] [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.
Default	no authentication-key
Parameters	<p><i>authentication-key</i> — 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 (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p><i>hash-key</i> — 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, enclose the entire string in quotation marks (" ").</p> <p>hash — specifies 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</p> <p>hash2 — specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable 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.</p>

igmp

Syntax	[no] igmp
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether IGMP protocol information should be synchronized with the multi-chassis peer.
Default	no igmp

igmp-snooping

Syntax	[no] igmp-snooping
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether IGMP snooping information should be synchronized with the multi-chassis peer.
Default	no igmp-snooping

local-dhcp-server

Syntax	[no] local-dhcp-server
Context	config>redundancy>multi-chassis>peer>sync
Description	This command synchronizes DHCP server information.
Default	no local-dhcp-server

mld-snooping

Syntax	[no] mld-snooping
Context	config>redundancy>multi-chassis>peer>sync
Description	This command is not supported. It is not blocked for backwards-compatibility reasons but has no effect on the system if configured.
Default	no mld-snooping

peer-name

Syntax	peer-name <i>name</i>
---------------	------------------------------

no peer-name

Context	config>redundancy>multi-chassis>peer
Description	This command specifies a peer name.
Default	no peer-name
Parameters	<i>name</i> — the string may be up to 32 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

pim-snooping

Syntax	pim-snooping [saps] no pim-snooping
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether PIM snooping for IPv4 information should be synchronized with the multi-chassis peer. Entering only pim-snooping (without any parameter) results in the synchronization being applicable only to SAPs.
Default	no pim-snooping
Parameters	<i>saps</i> — specifies that SAPs are to be synchronized with the multi-chassis peer relating to <i>sync-tags</i> configured on ports. This is the default when no parameters are included.

port

Syntax	port [port-id lag-id] [sync-tag sync-tag] no port [port-id lag-id]
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies the port to be synchronized with the multi-chassis peer and a synchronization tag to be used while synchronizing this port with the multi-chassis peer.
Default	N/A
Parameters	<i>port-id</i> — specifies the port to be synchronized with the multi-chassis peer <i>lag-id</i> — specifies the LAG ID to be synchronized with the multi-chassis peer sync-tag sync-tag — specifies a synchronization tag to be used while synchronizing this port with the multi-chassis peer

python

Syntax	python
Context	config>redundancy>multi-chassis>peer>sync
Description	<p>This command enables syncing of python-policy cached entries to the peer.</p> <p>Use the mcs-peer command in the python-policy to enable syncing for a specific python-policy.</p>
Default	no python

range

Syntax	range <i>encap-range</i> sync-tag <i>sync-tag</i> no range <i>encap-range</i>
Context	config>redundancy>multi-chassis>peer>sync>port
Description	This command configures a range of encapsulation values.
Parameters	<p><i>encap-range</i> — specifies a range of encapsulation values on a port to be synchronized with a multi-chassis peer</p> <p>Values Dot1Q <i>start-vlan-end-vlan</i> QinQQ1 <i>start-vlan-Q1.end-vlan</i></p> <p>sync-tag <i>sync-tag</i> — specifies a synchronization tag up to 32 characters in length to be used while synchronizing this encapsulation value range with the multi-chassis peer</p>

source-address

Syntax	source-address <i>ip-address</i> no source-address
Context	config>redundancy>multi-chassis>peer
Description	This command specifies the source address used to communicate with the multi-chassis peer.
Default	no source-address
Parameters	<i>ip-address</i> — specifies the source address used to communicate with the multi-chassis peer

srrp

Syntax	[no] srrp
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether subscriber routed redundancy protocol (SRRP) information should be synchronized with the multi-chassis peer.
Default	no srrp

sync

Syntax	[no] sync
Context	config>redundancy>multi-chassis>peer
Description	This command enables the context to configure synchronization parameters.
Default	N/A

sub-mgmt

Syntax	[no] sub-mgmt
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether subscriber management information should be synchronized with the multi-chassis peer.
Default	no sub-mgmt

sub-host-trk

Syntax	[no] sub-host-trk
Context	config>redundancy>multi-chassis>peer>sync
Description	This command specifies whether subscriber host tracking information should be synchronized with the multi-chassis peer.
Default	no sub-host-trk

warm-standby

Syntax	warm-standby
---------------	---------------------

Context	config>redundancy>multi-chassis>peer
Description	<p>This command enables Oversubscribed Multi-Chassis Redundancy (OMCR). Subscriber hosts are synchronized between two chassis only in the control plane and are kept there (as part of the Multi-Chassis Synchronization (MCS) state) until the switchover occurs. Link or nodal failure will trigger the switchover at which point the subscriber hosts are being fully instantiated in the control and the forwarding plane. This approach allows oversubscription of the resources in the central standby (or protecting) node that is backing-up a number of other active nodes. The total number of protected subscribers in the OMCR cluster exceeds the forwarding capacity of the protecting node. This is achievable by not fully occupying the resources for the subscriber hosts until the failure occurs.</p> <p>The restoration times depend on the amount of the subscriber hosts that are affected by the switchover and it is related to the time needed for the full instantiation of the subscribers in the forwarding plane.</p> <p>Although this command is configured on a peer level, the warm-standby property is a nodal characteristic. In other words, mixing of N:1 and 1:1 (hot standby) mode in the central standby node is not supported. Consequently all peers on the central standby node must be configured for warm-standby (N:1), or all peers must be configured for hot-standby (1:1) by omitting the warm-standby keyword from the configuration.</p> <p>The peer of the central-backup node is not aware of the redundancy model supported. In other words, the peer of the central-backup node does not know whether it peers with a warm-standby peer or host-standby-peer. All nodes participating in this protection model must run SR OS R12.0 or higher.</p> <p>This command applies only to the 7450 ESS and 7750 SR.</p>
Default	no warm-standby

5.22.2.14.2 Multi-Chassis Endpoint Commands

mc-endpoint

Syntax	[no] mc-endpoint
Context	config>redundancy>multi-chassis>peer
Description	<p>This command specifies that the endpoint is multi-chassis. This value should be the same on both MC-EP peers for the pseudowires that must be part of the same group.</p> <p>The no form of this command removes the endpoint from the MC-EP. Single chassis behavior applies.</p>
Default	no mc-endpoint

bfd-enable

Syntax	[no] bfd-enable
Context	config>redundancy>multi-chassis>peer>mc-ep config>router>rsvp config>router>bgp config>router>bgp>group config>router>bgp>group>neighbor config>redundancy>multi-chassis>peer>mc-ep
Description	<p>This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.</p> <p>The no form of this command disables BFD.</p>
Default	no bfd-enable

boot-timer

Syntax	boot-timer <i>interval</i> no boot-timer
Context	config>redundancy>multi-chassis>peer>mc-ep
Description	<p>This command configures the boot timer interval. This command applies only when the node reboots. It specifies the time the MC-EP protocol keeps trying to establish a connection before assuming a failure of the remote peer. This is different from the keep-alives mechanism which is used just after the peer-peer communication was established. After this time interval passed all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local PW.</p> <p>The no form of this command sets the interval to default.</p>
Default	boot-timer 300
Parameters	<i>interval</i> — specifies the boot timer interval
Values	1 to 600

hold-on-neighbor-failure

Syntax	hold-on-neighbor-failure <i>multiplier</i> no hold-on-neighbor-failure
Context	config>redundancy>multi-chassis>peer>mc-ep

Description	<p>This command specifies the number of keep-alive intervals that the local node will wait for packets from the MC-EP peer before assuming failure. After this time interval passed the all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local pseudowire.</p> <p>The no form of this command sets the multiplier to default value.</p>
Default	hold-on-neighbor-failure 3
Parameters	<i>multiplier</i> — specifies the hold time applied on neighbor failure
Values	2 to 25

keep-alive-interval

Syntax	keep-alive-interval <i>interval</i> no keep-alive-interval
Context	config>redundancy>multi-chassis>peer>mc-ep
Description	<p>This command sets the interval at which keep-alive messages are exchanged between two systems participating in MC-EP when bfd is not enabled or is down. These fast keep-alive messages are used to determine remote-node failure and the interval is set in deci-seconds.</p> <p>The no form of this command sets the interval to default value</p>
Default	keep-alive-interval 5 (0.5s)
Parameters	<i>interval</i> — the time interval expressed in deciseconds
Values	5 to 500 (tenths of a second)

passive-mode

Syntax	[no] passive-mode
Context	config>redundancy>multi-chassis>peer>mc-ep
Description	<p>This command configures the passive mode behavior for the MC-EP protocol. When in passive mode the MC-EP pair will be dormant until two of the pseudowires in a MC-EP will be signaled as active by the remote PEs, being assumed that the remote pair is configured with regular MC-EP. As soon as more than one pseudowire is active, dormant MC-EP pair will activate. It will use the regular exchange to select the best pseudowire between the active ones and it will block the Rx and Tx directions of the other pseudowires.</p> <p>The no form of this command will disable the passive mode behavior.</p>
Default	no passive-mode

system-priority

Syntax	system-priority <i>value</i> no system-priority
Context	config>redundancy>multi-chassis>peer>mc-ep
Description	This command allows the operator to set the system priority. The peer configured with the lowest value is chosen to be the master. If system-priority are equal then the one with the highest system-id (chassis MAC address) is chosen as the master. The no form of this command sets the system priority to default.
Default	no system-priority

5.22.2.14.3 MC-LAG Commands

mc-lag

Syntax	[no] mc-lag
Context	config>redundancy>multi-chassis>peer>mc-lag
Description	This command enables the context to configure multi-chassis LAG operations and related parameters. The no form of this command administratively disables multi-chassis LAG. MC-LAG can only be issued only when mc-lag is shutdown.
Default	N/A

hold-on-neighbor-failure

Syntax	hold-on-neighbor-failure <i>multiplier</i> no hold-on-neighbor-failure
Context	config>redundancy>multi-chassis>peer>mc-lag
Description	This command specifies the interval that the standby node will wait for packets from the active node before assuming a redundant-neighbor node failure. This delay in switch-over operation is required to accommodate different factors influencing node failure detection rate, such as IGP convergence, or HA switch-over times and to prevent the standby node to take action prematurely. The no form of this command sets this parameter to default value.
Default	hold-on-neighbor-failure 3

Parameters *multiplier* — the time interval 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 keep-alive messages are exchanged between two systems participating in MC-LAG. These keep-alive messages are used to determine remote-node failure and the interval is set in deciseconds.

The **no** form of this command sets the interval to default value

Default keep-alive-interval 1s (10 hundreds of milliseconds means interval value of 10)

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 remote-lag-id] system-priority system-priority source-bmac-lsb use-lacp-key*
lag *lag-id lacp-key admin-key system-id system-id [remote-lag remote-lag-id] system-priority system-priority source-bmac-lsb MAC-Lsb*
lag *lag-id lacp-key admin-key system-id system-id [remote-lag remote-lag-id] system-priority system-priority*
lag *lag-id [remote-lag remote-lag-id]*
no lag *lag-id*

Context config>redundancy>multi-chassis>peer>mc-lag

Description This command defines a LAG which 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 1 peer.

The same **lacp-key**, **system-id**, and **system-priority** must be configured on both nodes of the redundant pair in order to MC-LAG to become operational. In order MC-LAG to become operational, all parameters (**lacp-key**, **system-id**, **system-priority**) must be configured the same on both nodes of the same redundant pair.

The partner system (the system connected to all links forming MC-LAG) will consider all ports using the same **lacp-key**, **system-id**, **system-priority** as the part of the same LAG. In order to achieve this in MC operation, both redundant-pair nodes have to be configured with the same values. In case of the mismatch, MC-LAG is kept operationally down.

Default	N/A
Parameters	<p><i>lag-id</i> — the LAG identifier, expressed as a decimal integer. Specifying the <i>lag-id</i> allows the mismatch between lag-id on redundant-pair. If no lag-id is specified it is assumed that neighbor system uses the same <i>lag-id</i> as a part of the given MC-LAG. 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.).</p> <p>Values 1 to 800</p> <p>lACP-key <i>admin-key</i> — 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 come up</p> <p>Values 1 to 65535</p> <p>system-id <i>system-id</i> — specifies a 6 byte value expressed in the same notation as MAC address</p> <p>Values xx:xx:xx:xx:xx:xx - xx [00 to FF]</p> <p>remote-lag <i>lag-id</i> — specifies the LAG ID on the remote system</p> <p>Values 1 to 800</p> <p>system-priority <i>system-priority</i> — 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.</p> <p>Values 1 to 65535</p>

5.22.2.14.4 Multi-Chassis Ring Commands

mc-ring

Syntax	mc-ring
Context	config>redundancy>mc>peer config>redundancy>multi-chassis>peer>sync
Description	This command enables the context to configure the multi-chassis ring parameters.
Default	N/A

ring

Syntax	ring <i>sync-tag</i> no ring <i>sync-tag</i>
Context	config>redundancy>mc>peer>mcr

Description	This command configures a multi-chassis ring.
Default	N/A
Parameters	<i>sync-tag</i> — specifies a synchronization tag to be used while synchronizing this port with the multi-chassis peer

in-band-control-path

Syntax	in-band-control-path
Context	config>redundancy>mc>peer>mcr>ring
Description	This command enables the context to configure multi-chassis ring inband control path parameters.

dst-ip

Syntax	dst-ip <i>ip-address</i> no dst-ip
Context	config>redundancy>mc>peer>mcr>ring>in-band-control-path
Description	This command specifies the destination IP address used in the inband control connection. If the address is not configured, the ring cannot become operational.
Default	N/A
Parameters	<i>ip-address</i> — specifies the destination IP address

interface

Syntax	interface <i>ip-int-name</i> no interface
Context	config>redundancy>mc>peer>mcr>ring>in-band-control-path
Description	This command specifies the name of the IP interface used for the inband control connection. If the name is not configured, the ring cannot become operational.
Default	no interface

service-id

Syntax	service-id <i>service-id</i>
---------------	-------------------------------------

no service-id

Context	config>redundancy>mc>peer>mcr>ring>ibc
Description	This command specifies the service ID if the interface used for the inband control connection belongs to a VPRN service. If not specified, the <i>service-id</i> is zero and the interface must belong to the Base router. The no form of the command removes the service-id from the IBC configuration.
Default	no service-id
Parameters	<i>service-id</i> — specifies the service ID if the interface

path-b

Syntax	[no] path-b
Context	config>redundancy>mc>peer>mcr>ring
Description	This command specifies the set of upper-VLAN IDs associated with the SAPs that belong to path B with respect to load-sharing. All other SAPs belong to path A.
Default	If not specified, the default is an empty set.

range

Syntax	[no] range <i>vlan-range</i>
Context	config>redundancy>mc>peer>mcr>ring>path-b config>redundancy>mc>peer>mcr>ring>path-excl
Description	This command configures a MCR b-path VLAN range.
Default	no range
Parameters	<i>vla-range</i> — specifies the VLAN range Values <i>vla-range</i> — 1 to 4094

path-excl

Syntax	[no] path-excl
Context	config>redundancy>mc>peer>mcr>ring
Description	This command specifies the set of upper-VLAN IDs associated with the SAPs that are to be excluded from control by the multi-chassis ring.

Default If not specified, the default is an empty set.

ring-node

Syntax **ring-node** *ring-node-name* [**create**]
no ring-node *ring-node-name*

Context config>redundancy>mc>peer>mcr>ring

Description This command specifies the unique name of a multi-chassis ring access node.

Default N/A

Parameters *ring-node-name* — specifies the unique name of a multi-chassis ring access node
create — keyword used to create the ring node instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

connectivity-verify

Syntax **connectivity-verify**

Context config>redundancy>mc>peer>mcr>ring>ring-node

Description This command enables the context to configure node connectivity check parameters.

Default N/A

dst-ip

Syntax **dst-ip** *ip-address*
no dst-ip

Context config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify

Description This command configures the node cc destination IP address.

Default no dst-ip

Parameters *ip-address* — specifies the destination IP address used in the inband control connection

interval

Syntax **interval** *interval*
no interval

Context	config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify
Description	This command specifies the polling interval of the ring-node connectivity verification of this ring node.
Default	interval 5
Parameters	<i>interval</i> — specifies the polling interval, in minutes
Values	1 to 6000

service-id

Syntax	service-id <i>service-id</i> no service-id
Context	config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify
Description	This command specifies the service ID of the SAP used for the ring-node connectivity verification of this ring node.
Default	no service-id
Parameters	<i>service-id</i> — specifies the service ID of the SAP
Values	1 to 2147483647

src-ip

Syntax	src-ip <i>ip-address</i> no src-ip
Context	config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify
Description	This command specifies the source IP address used in the ring-node connectivity verification of this ring node.
Default	no src-ip
Parameters	<i>ip-address</i> — specifies the address of the multi-chassis peer

src-mac

Syntax	src-mac <i>ieee-address</i> no src-mac
Context	config>redundancy>mc>peer>mcr>node>cv

Description	This command specifies the source MAC address used for the Ring-Node Connectivity Verification of this ring node. A value of all zeros (000000000000 H (0:0:0:0:0:0)) specifies that the MAC address of the system management processor (CPM) is used.
Default	no src-mac
Parameters	<i>ieee-address</i> — specifies the source MAC address

5.22.2.15 LLDP System Commands

lldp

Syntax	lldp
Context	config>system
Description	This command enables the context to configure system-wide Link Layer Discovery Protocol parameters.
Default	N/A

message-fast-tx

Syntax	message-fast-tx <i>time</i> no message-fast-tx				
Context	config>system>lldp				
Description	This command configures the duration of the fast transmission period.				
Default	no message-fast-tx				
Parameters	<i>time</i> — specifies the fast transmission period in seconds <table><tr><td>Values</td><td>1 to 3600</td></tr><tr><td>Default</td><td>1</td></tr></table>	Values	1 to 3600	Default	1
Values	1 to 3600				
Default	1				

message-fast-tx-init

Syntax	message-fast-tx-init <i>count</i> no message-fast-tx-init
Context	config>system>lldp

Description	This command configures the number of LLDPDUs to send during the fast transmission period.
Default	no message-fast-tx-init
Parameters	<i>count</i> — specifies the number of LLDPDUs to send during the fast transmission period
Values	1 to 8
Default	4

notification-interval

Syntax	notification-interval <i>time</i> no notification-interval
Context	config>system>lldp
Description	This command configures the minimum time between change notifications.
Default	no notification-interval
Parameters	<i>time</i> — specifies the minimum time, in seconds, between change notifications
Values	5 to 3600
Default	5

reinit-delay

Syntax	reinit-delay <i>time</i> no reinit-delay
Context	config>system>lldp
Description	This command configures the time before re-initializing LLDP on a port.
Default	no reinit-delay
Parameters	<i>time</i> — specifies the time, in seconds, before re-initializing LLDP on a port
Values	1 to 10
Default	2

tx-credit-max

Syntax	tx-credit-max <i>count</i> no tx-credit-max
---------------	--

Context	config>system>lldp
Description	This command configures the maximum consecutive LLDPDUs transmitted.
Default	no tx-credit-max
Parameters	<i>count</i> — specifies the maximum consecutive LLDPDUs transmitted
Values	1 to 100
Default	5

tx-hold-multiplier

Syntax	tx-hold-multiplier <i>multiplier</i> no tx-hold-multiplier
Context	config>system>lldp
Description	This command configures the multiplier of the tx-interval.
Default	no tx-hold-multiplier
Parameters	<i>multiplier</i> — specifies the multiplier of the tx-interval
Values	2 to 10
Default	4

tx-interval

Syntax	tx-interval <i>interval</i> no tx-interval
Context	config>system>lldp
Description	This command configures the LLDP transmit interval time.
Default	no tx-interval
Parameters	<i>interval</i> — specifies the LLDP transmit interval time
Values	1 to 100
Default	5

5.22.2.16 LLDP Ethernet Port Commands

lldp

Syntax	lldp
Context	config>port>ethernet
Description	This command enables the context to configure Link Layer Discovery Protocol (LLDP) parameters on the specified port.
Default	N/A

dest-mac

Syntax	dest-mac { <i>bridge-mac</i> }
Context	config>port>ethernet>lldp
Description	This command configures destination MAC address parameters.
Default	N/A
Parameters	bridge-mac — specifies destination bridge MAC type to use by LLDP
Values	nearest-bridge — specifies to use the nearest bridge nearest-non-tpmr — specifies to use the nearest non-Two-Port MAC Relay (TPMR) nearest-customer — specifies to use the nearest customer

admin-status

Syntax	admin-status { <i>rx</i> <i>tx</i> <i>tx-rx</i> disabled }
Context	config>port>ethernet>lldp>dstmac
Description	This command specifies the administratively desired status of the local LLDP agent.
Parameters	rx — specifies the LLDP agent will receive, but will not transmit LLDP frames on this port tx — specifies that the LLDP agent will transmit LLDP frames on this port and will not store any information about the remote systems connected tx-rx — specifies that the LLDP agent will transmit and receive LLDP frames on this port

disabled — specifies that the LLDP agent will not transmit or receive LLDP frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port's admin status becomes disabled, then the information will naturally age out.

notification

Syntax	[no] notification
Context	config>port>ethernet>lldp>dstmac
Description	This command enables LLDP notifications. The no form of the command disables LLDP notifications.

tx-mgmt-address

Syntax	tx-mgmt-address [system] no tx-mgmt-address
Context	config>port>ethernet>lldp>dstmac
Description	This command specifies which management address to transmit. The no form of the command resets value to the default.
Default	no tx-mgmt-address
Parameters	system — specifies to use the system IP address. The system address will only be transmitted once it has been configured if this parameter is specified

tx-tlvs

Syntax	tx-tlvs [port-desc] [sys-name] [sys-desc] [sys-cap] no tx-tlvs
Context	config>port>ethernet>lldp>dstmac
Description	This command specifies which LLDP TLVs to transmit. The no form of the command resets the value to the default.
Default	no tx-tlvs
Parameters	port-desc — indicates that the LLDP agent should transmit port description TLVs sys-name — indicates that the LLDP agent should transmit system name TLVs

sys-desc — indicates that the LLDP agent should transmit system description TLVs

sys-cap — indicates that the LLDP agent should transmit system capabilities TLVs

5.22.2.17 Optical Extension Shelf (OES) Commands



Note: OES commands are only applicable to the 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7950 XRS-20, and 7950 XRS-40 routers.

oes

Syntax	oes
Context	config>system
Description	This command creates or edits the context in which to configure the OES subsystem.

cf-cache

Syntax	cf-cache <i>cf-flash-id</i>
Context	config>system>oes
Description	This command designates the compact flash to use for the cache for OES operations. The cache is used to store diagnostic information and as a temporary location for software files during an OES upgrade operation.
Default	cf-cache cf3
Parameters	<i>cf-flash-id</i> — specifies the Cflash ID
Values	cf1, cf2, cf3

chassis

Syntax	chassis <i>chassis-id</i> type <i>type</i> create no chassis
Context	config>system>oes
Description	This command creates a chassis in the OES subsystem. A chassis must be created before any cards or ports can be referenced. The no form of the command removes the chassis configuration.

Default	no chassis
Parameters	<i>chassis-id</i> — specifies the OES chassis ID
Values	oes-1
	<i>type</i> — specifies the type of OES chassis
Values	pss32

description

Syntax	description <i>description-string</i> no description
Context	config>system>oes>chassis
Description	This command defines a description string for the OES chassis. The no form of the command deletes the associated description string.
Default	no description
Parameters	<i>description-string</i> — specifies the OES chassis description, up to 80 characters in length

fan-speed

Syntax	fan-speed { normal maximum }
Context	config>system>oes>chassis
Description	This command sets the fan speed on the OES chassis. The fan speed should be set to normal except during certain maintenance operations.
Default	fan-speed normal
Parameters	normal maximum — specifies the fan speed
Values	normal — The fan speed is controlled automatically by the system during normal operation. maximum — The fan runs at a constant full speed during maintenance operations.

control-communications

Syntax	control-communications
Context	config>system>oes

Description This command creates or edits the context in which to configure the control communication parameters for an OES subsystem.

Control communications comprise a set of parameters for the internal control communications between the router and the OES. Separate subnets are required for each of the two physical control communication links between the router (that is, the OES ports on the CCM/CPM) and the OES master chassis (that is, the AUX ports on the EC cards). The subnets and addresses must be reserved/allocated in a user-created CPM router instance and the same subnets and addresses can be used for all OES systems in the same network. These internal addresses are not externally reachable except through the OES ports). The CPM A OES port A/4 must be cabled to the AUX interface/port on the first (lowest slot number) EC card on the OES Master Chassis. The interface bound to A/4 and the AUX interface on the first EC card must belong to the same subnet. Similarly, the B/4 and the AUX port must be cabled on the second EC card.

oes-address

Syntax [no] **oes-address** *ip-address*

Context config>system>oes>ctrl-comm

Description This command configures the OES destination IP address (loopback address on the OES master chassis) to be used for OES control communication. This is the address to which OES control packets are transmitted.

This address must be reachable in the router instance configured under **configure system oes control-communications router** *cpm-vr-name*; for example, by configuring static routes in the router instance that direct traffic out of the interfaces associated with the OES ports A/4 and B/4. If the OES address is not reachable, then the tmnxOesCtlCommsDown facility alarm will be raised. It is recommended to use the default loopback address of the OES: 172.16.1.1.

Parameters *ip-address* — specifies the OES destination IP address

router

Syntax [no] **router** *cpm-vr-name*

Context config>system>oes>ctrl-comm

Description This command configures the user-created CPM router instance to be used for OES control communication.

Default no router

Parameters *cpm-vr-name* — specifies the CPM router instance name, up to 32 characters

retry-limit

Syntax	retry-limit <i>retry_num</i>
Context	config>system>oes>ctrl-comm
Description	This command specifies the number of attempts that can be made to re-establish communication with the OES. The OES is declared unreachable if a timeout occurs for consecutive retry limit attempts, that is, after (timeout * (retry-limit + 1)) seconds.
Parameters	<i>retry_num</i> — specifies the number of attempts the router can make to re-establish communication with the OES
Values	0 to 7
Default	2

timeout

Syntax	timeout <i>seconds</i>
Context	config>system>oes>ctrl-comm
Description	This command specifies the timeout for communications to the OES chassis.
Parameters	<i>seconds</i> — specifies the amount of time, in seconds, for the communications timeout to the OES chassis
Values	5 to 3600
Default	20 (for the SNMP keep alive)

software-repository

Syntax	software-repository <i>repository-name</i> no software-repository
Context	config>system>oes
Description	<p>This command binds the specified software repository to the OES subsystem. The software repository is used to upgrade the software running on the OES chassis.</p> <p>The software repository supports multiple locations. If more than one location is specified, it is important to ensure each location has the required software load. For the complete OES software upgrade procedure, see the 7750 SR and 7950 XRS Optical Extension Shelf (OES) Installation Guide.</p> <p>The no form of the command removes the software repository.</p>
Default	no software-repository

5.23 Show, Clear, Debug, and Tools Command Reference

5.23.1 Command Hierarchies

- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)
- [Tools Commands](#)

5.23.1.1 Show Commands

```

show
  — redundancy
    — mgmt-ethernet
    — multi-chassis
      — all [detail]
      — mc-endpoint statistics
      — mc-endpoint peer [ip-address] statistics
      — mc-endpoint endpoint [mcep-id] statistics
      — mc-endpoint peer [ip-address]
      — mc-lag [lag lag-id]
        — peer [peer ip-address [lag lag-id]] mc-lag
        — statistics
      — mc-ring peer ip-address statistics
      — mc-ring peer ip-address [ring sync-tag [detail | statistics]]
      — mc-ring peer ip-address ring sync-tag ring-node [ring-node-name [detail |
        statistics]]
      — mc-ring global-statistics
      — sync [port port-id | lag-id]
        — peer [port port-id]
        — detail
    — synchronization
  — time
  — system
    — alarm-contact-input {alarm-contact-input-id | all} [detail]
    — card
      — cpu [sample-period seconds]
      — memory-pools
    — connections [address ip-address [interface interface-name]] [port port-number]
      [detail]
    — cpu [sample-period seconds]
    — cron
      — action
      — schedule
    — information
    — lldp neighbor
    — load-balancing-alg [detail]
    — memory-pools
    — ntp
    — oes
    — port-topology [uni-dir]
    — ptp [standby]
    — ptp peers [router router-instance | service-name service-name] [detail]
    — ptp port
    — ptp port port-id [detail]
    — ptp statistics
    — ptp unicast [router router-instance | service-name service-name]
    — rollback
    — satellite
    — script-control
      — script [script-name] [owner script-owner]
      — script-policy script-policy-name [owner owner-name]

```

- **script-policy** run-history [*run-state*]
- **sntp**
- **switch-fabric** [exclude-sfm *sfm-list*]
- **switch-fabric** high-bandwidth-multicast
- **sync-if-timing**
- **thresholds**
- **time**
- uptime

5.23.1.2 Clear Commands

- clear
- **application-assurance**
 - **group** *isa-aa-group-id* statistics
 - **group** *isa-aa-group-id* status
 - **redundancy**
 - **multi-chassis**
 - **mc-endpoint** endpoint [*mcep-id*] statistics
 - **mc-endpoint** statistics
 - **mc-endpoint** peer [*ip-address*] statistics
 - **mc-lag** [peer *ip-address* [*lag lag-id*]]
 - **mc-ring**
 - **debounce** peer *ip-address* ring *sync-tag*
 - **ring-nodes** peer *ip-address* ring *sync-tag*
 - **statistics**
 - **global**
 - **peer** *ip-address*
 - **ring** peer *ip-address* ring *sync-tag*
 - **ring-node** peer *ip-address* ring *sync-tag* node *ring-node-name*
 - **sync-database** peer *ip-address* all application *application*
 - **sync-database** peer *ip-address* {port *port-id* | *lag-id* | **sync-tag** *sync-tag*} application *application*
 - **sync-database** peer *ip-address* {sdp *sdp-id* | **sync-tag** *sync-tag*} application *application*
 - **sync-database** peer *ip-address* **sync-tag** *sync-tag* application *application*
 - **screen**
 - **system**
 - **ptp**
 - **inactive-peers**
 - **peer** *ip-address* [router *router-instance*] statistics
 - **port** *port-id* statistics
 - **statistics**
 - **script-control**
 - **script-policy**
 - **completed** [*script-policy-name*] [owner *owner-name*]
 - **statistics**
 - **xmpp** *xmpp-server-name*
 - **sync-if-timing** {ref1 | ref2 | bits}

5.23.1.3 Debug Commands

```

debug
— sync-if-timing
  — force-reference {ref1 | ref2 | bits | bits1 | bits2 | bitsa | bitsb | ptp}
  — no force-reference
— [no] system
  — http-connections [host-ip-address/mask]
  — no http-connections
  — ntp [router router-name] [interface ip-int-name]
  — persistence

```

5.23.1.4 Tools Commands

```

tools
— dump
  — redundancy
    — multi-chassis
      — mc-endpoint peer ip-address
      — mc-ring
      — mc-ring peer ip-address [ring sync-tag]
      — srrp-sync-database [instance instance-id] [peer ip-address]
      — sync-database [peer ip-address] [port port-id | lag-id] [sync-tag sync-tag] [application application] [detail] [type type]
    — resource-usage
      — card [slot-num]
      — card [slot-num] all
        — fp [fp-number]
        — mda [mda-slot]
      — system [all]
    — system-resources slot-number
  — perform
    — redundancy
      — mgmt-ethernet
    — chassis
      — set-role {standalone | master | extension}
    — system
      — inter-chassis
        — sfm-interco-test [sfm x]
        — mixed-mode-upgrade [slot-list] [now]
  — perform
    — system
      — script-control
        — script-policy
          — stop [script-policy-name] [owner script-policy-owner] [all]
      — set-fabric-speed speed
      — cron

```

5.23.2 Command Descriptions

5.23.2.1 Show Commands

The command outputs in the following sections are examples only; actual displays may differ depending on supported functionality and user configuration.

alarm-contact-input

- Syntax** `alarm-contact-input {alarm-contact-input-id | all} [detail]`
- Context** `show>system`
- Description** This command displays the alarm contact input information.
- Parameters** *alarm-contact-input-id* — displays the alarm contact input information for a specific pin
- Values** 1 to 4
- all** — displays the alarm contact input information for all pins
- detail** — displays detailed alarm contact input information for one or all of the pins
- Output** The following table describes the system connections output fields.

Table 45 Alarm Contact Input Field Descriptions

Label	Description
Alarm Contact Input Power	Indicates if the +24VDC output pin (optionally used to provide power for the alarm inputs) is enabled
Current State	Indicate the configured administrative state of the input Disabled = the alarm-contact-input is disabled (shutdown) and log events will not be generated for changes to the input pin status Enabled = the alarm-contact-input is enabled (no shutdown) and log events will be generated for changes to the input pin status (as long as the log events are not suppressed in event-control configuration)
Alarm Output Pin Used	Indicates the configured severity of the associated CHASSIS log event (for example, for pin 3: "configure log event-control" chassis" tmnxSasAlarminput3StateChanged)
Alarm Raised	Indicates if the input pin is 'triggered' or not
Last State Change	Indicates when the input pin last changed state

Sample Output

```
A:bkvm3# show system alarm-contact-input 1
```

```
=====
Alarm Contact Input
=====
Alarm Contact Input Power          : on
Alarm Input Pin Number            : 1
    Alarm Input Pin Current State  : Disabled
    Alarm Output Pin Used          : major
    Alarm Raised                   : No
=====
```

```
A:bkvm3# show system alarm-contact-input 1 detail
```

```
=====
Alarm Contact Input
=====
Alarm Contact Input Power          : on
Alarm Input Pin Number            : 2
    Description                   : (Not Specified)
    Alarm Input Pin Current State  : Enabled
    Alarm Output Pin Used          : major
    Alarm Raised                   : No
    Last State Change             : 12/15/2014 13:11:32
=====
```

```
A:bkvm3# show system alarm-contact-input all
```

```
=====
Alarm Contact Input
=====
Alarm Contact Input Power          : on
Alarm Input Pin Number            : 1
    Description                   : cabinet door
    Alarm Input Pin Current State  : Enabled
    Alarm Output Pin Used          : major
    Alarm Raised                   : Yes
    Last State Change             : 12/17/2014 20:12:02
Alarm Input Pin Number            : 2
    Description                   : (Not Specified)
    Alarm Input Pin Current State  : Disabled
    Alarm Output Pin Used          : minor
    Alarm Raised                   : No
    Last State Change             : 12/17/2014 20:12:02
Alarm Input Pin Number            : 3
    Description                   : (Not Specified)
    Alarm Input Pin Current State  : Disabled
    Alarm Output Pin Used          : major
    Alarm Raised                   : No
    Last State Change             : 12/17/2014 20:12:02
Alarm Input Pin Number            : 4
    Description                   : (Not Specified)
    Alarm Input Pin Current State  : Disabled
    Alarm Output Pin Used          : critical
    Alarm Raised                   : No
    Last State Change             : 12/17/2014 20:12:02
=====
```


card

Syntax	card
Context	show>system
Description	This command enables the context to display card information.

memory-pools

Syntax	memory-pools
Context	show>system>card
Description	This command displays the memory pools for the card.

connections

Syntax	connections [address <i>ip-address</i>] [port <i>port-number</i>] [detail]												
Context	show>system												
Description	<p>This command displays UDP and TCP connection information.</p> <p>If no command line options are specified, a summary of the TCP and UDP connections displays.</p>												
Parameters	<p><i>ip-address</i> — Displays only the connection information for the specified IP address.</p> <p>Values</p> <table><tr><td>ipv4-address:</td><td>a.b.c.d (host bits must be 0)</td></tr><tr><td>ipv6-address:</td><td>x:x:x:x:x:x:x[-interface]</td></tr><tr><td></td><td>x:x:x:x:x:x:d.d.d.d[-interface]</td></tr><tr><td>x:</td><td>[0 to FFFF]H</td></tr><tr><td>d:</td><td>[0 to 255]D</td></tr><tr><td>interface:</td><td>32 characters maximum, mandatory for link local addresses</td></tr></table> <p><i>port-number</i> — Displays only the connection information for the specified port number.</p> <p>Values 0 to 65535</p> <p>detail — Appends TCP statistics to the display output.</p>	ipv4-address:	a.b.c.d (host bits must be 0)	ipv6-address:	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 characters maximum, mandatory for link local addresses
ipv4-address:	a.b.c.d (host bits must be 0)												
ipv6-address:	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 characters maximum, mandatory for link local addresses												
Output	The following table describes the system connections output fields.												

Table 46 **System Connections Field Descriptions**

Label	Description
Proto	Displays the socket protocol, either TCP or UDP.
RecvQ	Displays the number of input packets received by the protocol.
TxmtQ	Displays the number of output packets sent by the application.
Local Address	Displays the local address of the socket. The socket port is separated by a period.
Remote Address	Displays the remote address of the socket. The socket port is separated by a period.
State	Listen — The protocol state is in the listen mode.
	Established — The protocol state is established.
	vRtrID — The virtual router identifier. <ul style="list-style-type: none"> • 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
	MSS — The TCP maximum segment size.

Sample Output

```

A:ALA-12# show system connections
=====
Connections
=====
Prot RecvQ  TxmtQ  Local Address      State
      MSS   Remote Address      vRtrID
-----
TCP      0      0 0.0.0.0.21          LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 0.0.0.0.22          LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 0.0.0.0.23          LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 0.0.0.0.830         LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 0.0.0.0.6068        LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 0.0.0.0.47806       LISTEN
      1024 0.0.0.0.0           0
TCP      0      0 ::.21              LISTEN
      1024 ::.0                0
TCP      0      0 ::.22              LISTEN
      1024 ::.0                0
TCP      0      0 ::.830             LISTEN
      1024 ::.0                0

```

```

TCP      0      0  ::.47806                                LISTEN
      1024  ::.0                                0
TCP      0      0  127.1.0.11.21                            LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  127.1.0.11.21059                        LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  135.121.129.98.22                      LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  135.121.129.98.23                      ESTABLISH
      1024  138.120.140.149.59042                    4095
TCP      0      1149 135.121.129.98.23                    ESTABLISH
      1024  138.120.140.244.58579                    4095
TCP      0      0  135.121.129.98.830                    LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  3000::8779:8163.22                    LISTEN
      1024  ::.0                                4095
TCP      0      0  3000::8779:8163.830                    LISTEN
      1024  ::.0                                4095
UDP      0      0  0.0.0.0.67                            ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.68                            ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.123                          ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.319                          ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.320                          ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.514                          ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.50055                        ---
      0.0.0.0.0                                0
UDP      0      0  ::.123                                ---
      ::.0                                0
UDP      0      0  ::.50056                                ---
      ::.0                                0
UDP      0      0  0.0.0.0.1025                          ---
      0.0.0.0.0                                1
UDP      0      0  0.0.0.0.123                          ---
      0.0.0.0.0                                4095
UDP      0      0  0.0.0.0.49152
-----
No. of Connections: 18
=====
A:ALA-12#

```

Sample Detailed Output

A:ALA-12# 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:ALA-12#
```

cpu

Syntax	cpu [<i>sample-period seconds</i>]
Context	show>system show>card
Description	This command displays CPU utilization per task over a sample period.
Parameters	sample-period <i>seconds</i> — The number of seconds over which to sample CPU task utilization. Default 1 Values 1 to 300
Output	The following table describes the system CPU output fields.

Table 47 **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 each process or protocol has used in the specified time.
CPU Usage	The sum of CPU usage of all the processes and protocols.
Capacity Usage	<p>Displays the level the specified service is being utilized. When this number hits 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.</p> <p>This column does not reflect the true CPU utilization value; that data is still available in the CPU Usage column. This column is the busiest task in each group, where busiest is defined as either actually running or blocked attempting to acquire a lock.</p>

Sample Output

```
*A:cses-E11# show system cpu sample-period 2
=====
CPU Utilization (Sample period: 2 seconds)
=====
Name                               CPU Time      CPU Usage      Capacity
                                (uSec)                               Usage
-----
BFD                                10            ~0.00%         ~0.00%
BGP                                0             0.00%          0.00%
CFLOWD                             61            ~0.00%         ~0.00%
Cards & Ports                       8,332          0.41%          0.08%
DHCP Server                         79            ~0.00%         ~0.00%
ICC                                 408            0.02%          0.01%
IGMP/MLD                           1,768          0.08%          0.08%
IOM                                17,197         0.85%          0.31%
IP Stack                           4,080          0.20%          0.09%
IS-IS                              1,213          0.06%          0.06%
ISA                                 2,496          0.12%          0.07%
LDP                                 0             0.00%          0.00%
Logging                             32            ~0.00%         ~0.00%
MPLS/RSVP                          2,380          0.11%          0.08%
MSDP                                0             0.00%          0.00%
Management                         5,969          0.29%          0.15%
OAM                                 907            0.04%          0.02%
OSPF                                25            ~0.00%         ~0.00%
PIM                                 5,600          0.27%          0.27%
RIP                                 0             0.00%          0.00%
RTM/Policies                        0             0.00%          0.00%
Redundancy                         3,635          0.18%          0.13%
SIM                                 1,462          0.07%          0.04%
SNMP Daemon                        0             0.00%          0.00%
```

Services	2,241	0.11%	0.05%
Stats	0	0.00%	0.00%
Subscriber Mgmt	2,129	0.10%	0.04%
System	8,802	0.43%	0.17%
Traffic Eng	0	0.00%	0.00%
VRRP	697	0.03%	0.02%
WEB Redirect	125	~0.00%	~0.00%

Total	2,014,761	100.00%	
Idle	1,945,113	96.54%	
Usage	69,648	3.45%	
Busiest Core Utilization	69,648	3.45%	
=====			
*A:cses-E11#			
*A:ALA-1# show card 4 cpu			
=====			
Card 4 CPU Utilization (Sample period: 1 second)			
=====			
Name	CPU Time	CPU Usage	Capacity
	(uSec)		Usage

HQoS Algorithm	70	~0.00%	~0.00%
HQoS Statistics	124	~0.00%	0.83%
IOM	15,904	0.79%	0.94%

Total	2,003,678	100.00%	
Idle	1,987,580	99.19%	
Usage	16,098	0.80%	
Busiest Core Utilization	8,192	0.81%	
=====			

cron

Syntax	cron
Context	show>cron
Description	This command enters the show CRON context.

action

Syntax	action [<i>action-name</i>] [owner <i>action-owner</i>] run-history <i>run-state</i>
Context	show>cron
Description	This command displays cron action parameters.
Parameters	action <i>action-name</i> — Specifies the action name.
	Values maximum 32 characters

owner *action-owner* — Specifies the owner name.

Default TiMOS CLI

run-history *run-state* — Specifies the state of the test to be run.

Values executing, initializing, terminated

Output The following table describes the show cron action output fields.

Table 48 Cron Action Field Descriptions

Label	Description
Action	Displays the name of the action.
Action owner	The name of the action owner.
Administrative status	Enabled — Administrative status is enabled Disabled — Administrative status is disabled
Script	The name of the script
Script owner	The name of the script owner.
Script source location	Displays the location of scheduled script.
Max running allowed	Displays the maximum number of allowed sessions.
Max completed run histories	Displays the maximum number of sessions previously run.
Max lifetime allowed	Displays the maximum amount of time the script may run.
Completed run histories	Displays the number of completed sessions.
Executing run histories	Displays the number of sessions in the process of executing.
Initializing run histories	Displays the number of sessions ready to run/queued but not executed.
Max time run history saved	Displays the maximum amount of time to keep the results from a script run.
Last change	Displays the system time a change was made to the configuration.

Sample Output

```
*A:Redundancy# show cron action run-history terminated
=====
CRON Action Run History
=====
Action "test"
```

```

Owner "TiMOS CLI"
-----
Script Run #17
-----
Start time      : 2006/11/06 20:30:09      End time       : 2006/11/06 20:35:24
Elapsed time    : 0d 00:05:15             Lifetime      : 0d 00:00:00
State          : terminated                Run exit code  : noError
Result time     : 2006/11/06 20:35:24     Keep history   : 0d 00:49:57
Error time      : never
Results file    : ftp://*:*@192.168.15.18/home/testlab_bgp/cron/_20061106-203008.
                  out
Run exit        : Success
-----
Script Run #18
-----
Start time      : 2006/11/06 20:35:24      End time       : 2006/11/06 20:40:40
Elapsed time    : 0d 00:05:16             Lifetime      : 0d 00:00:00
State          : terminated                Run exit code  : noError
Result time     : 2006/11/06 20:40:40     Keep history   : 0d 00:55:13
Error time      : never
Results file    : ftp://*:*@192.168.15.18/home/testlab_bgp/cron/_20061106-203523.
                  out
Run exit        : Success
-----
*A:Redundancy#

*A:Redundancy# show cron action run-history executing
=====
CRON Action Run History
=====
Action "test"
Owner "TiMOS CLI"
-----
Script Run #20
-----
Start time      : 2006/11/06 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/_20061106-204559.
                  out
=====
*A:Redundancy#

*A:Redundancy# show cron action run-history initializing
=====
CRON Action Run History
=====
Action "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:Redundancy#
```

schedule

- Syntax** `schedule [schedule-name] [owner schedule-owner]`
- Context** `show>cron`
- Description** This command displays cron schedule parameters.
- Parameters**
 - schedule-name* — Displays information for the specified scheduler name.
 - owner schedule-owner* — Displays information for the specified scheduler owner.
- Output** The following table describes the show cron schedule output fields.

Table 49 Cron Schedule Field Descriptions

Label	Description
Schedule name	Displays the schedule name.
Schedule owner	Displays the owner name of the action.
Description	Displays the schedule's description.
Administrative status	Enabled — The administrative status is enabled.
	Disabled — Administratively disabled.
Operational status	Enabled — The operational status is enabled.
	Disabled — Operationally disabled.

Table 49 Cron Schedule Field Descriptions (Continued)

Label	Description (Continued)
Action	Displays the action name
Action owner	Displays the name of action owner.
Script	Displays the name of the script.
Script owner	Displays the name of the script.
Script owner	Displays the name of the of script owner.
Script source location	Displays the location of scheduled script.
Script results location	Displays the location where the script results have been sent.
Schedule type	Periodic — Displays a schedule which ran at a given interval. Calendar — Displays a schedule which ran based on a calendar. Oneshot — Displays a schedule which ran one time only.
Interval	Displays the interval between runs of an event.
Next scheduled run	Displays the time for the next scheduled run.
Weekday	Displays the configured weekday.
Month	Displays the configured month.
Day of Month	Displays the configured day of month.
Hour	Displays the configured hour.
Minute	Displays the configured minute.
Number of scheduled runs	Displays the number of scheduled sessions.
Last scheduled run	Displays the last scheduled session.
Number of scheduled failures	Displays the number of scheduled sessions that failed to execute.
Last scheduled failure	Displays the last scheduled session that failed to execute.
Last failure time	Displays the system time of the last failure.

Sample Output

```
A:siml>show>cron schedule test
```

```
=====
```

```
CRON Schedule Information
=====
Schedule                : test
Schedule owner          : TiMOS CLI
Description              : none
Administrative status    : enabled
Operational status      : enabled
Action                  : test
Action owner            : TiMOS CLI
Script                  : test
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)
Next scheduled run       : 0d 00:00:42
Weekday                  : tuesday
Month                    : none
Day of month             : none
Hour                     : none
Minute                   : none
Number of schedule runs  : 10
Last schedule run        : 2008/01/01 17:20:52
Number of schedule failures : 0
Last schedule failure    : no error
Last failure time        : never
=====
A:sim1>show>cron
```

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 table describes the system information output fields.

Table 50 **System Information Field Descriptions**

Label	Description
System Name	The configured system name.
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.

Table 50 **System Information Field Descriptions (Continued)**

Label	Description (Continued)
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 engineID to uniquely identify the SNMPv3 node.
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 shutdown 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.
Telnet/SSH/FTP Admin	Displays the administrative state of the Telnet, SSH, and FTP sessions.
Telnet/SSH/FTP Oper	Displays the operational state of the Telnet, 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. 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.
DNS Resolve Preference	ipv4-only — Dns-names are queried for A-records only. ipv6-first — Dns-server will be queried for AAAA-records first and a successful reply is not received, the dns-server is queried for A-records.
Last Booted Config File	The URL and filename of the last loaded configuration file.

Table 50 System Information Field Descriptions (Continued)

Label	Description (Continued)
Last Boot Cfg Version	The date and time of the last boot.
Last Boot Config Header	Displays header information such as image version, date built, date generated.
Last Boot Index Version	The version of the persistence index file read when this card was last rebooted.
Last Boot Index Header	The header of the persistence index file read when this 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.
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.
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.
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.
Management IP Addr	The management IP address and mask.
DNS Server	The IP address of the DNS server.
DNS Domain	The DNS domain name of the node.

Table 50 **System Information Field Descriptions (Continued)**

Label	Description (Continued)
BOF Static Routes	<p>To — The static route destination.</p> <p>Next Hop — The next hop IP address used to reach the destination.</p> <p>Metric — Displays the priority of this static route versus other static routes.</p> <p>None — No static routes are configured.</p>

Sample Output

```
A:Dut-F>show system information
...
Primary DNS Server      : 138.120.252.56
Secondary DNS Server    : 138.120.252.48
Tertiary DNS Server     : 138.120.252.49
DNS Domain              : labs.ca.nokia.com
DNS Resolve Preference : ipv4-only
DNSSEC                  AD Validated      : False
DNSSEC Response Control: drop
BOF Static Routes       :
```

The following is an example of the 7750 SR:

```
A:Dut-F# show system information
=====
System Information
=====
System Name           : Dut-F
System Type           : 7750 SR-7 7450 ESS-7
System Version        : B-6.0.B1-6
System Contact        :
System Location       :
System Coordinates    :
System Active Slot    : A
System Up Time        : 0 days, 03:42:01.29 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f00008c6cff000000
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            : ftp://test:test@xxx.xxx.xx.xxx/./images
Image Source          : primary
Config Source         : primary
Last Booted Config File: ftp://*:~@xxx.xxx.xx.xxx/./images/dut-f.cfg
Last Boot Cfg Version : N/A
Last Boot Index Version: N/A
```

```

Last Saved Config      : N/A
Time Last Saved       : N/A
Changes Since Last Save: No
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script         : ftp://*: *[3000::8acb:466d]/./images/env.cfg
Cfg-OK Script Status   : failed
Cfg-Fail Script        : N/A
Cfg-Fail Script Status : not used
Management IP Addr     : xxx.xxx.xx.xxx/23
Primary DNS Server     : xxx.xxx.xx.xxx
Secondary DNS Server   : xxx.xxx.xx.xxx
Tertiary DNS Server    : N/A
DNS Domain             : sh.bel.nokia.be
DNS Resolve Preference : ipv4-only
BOF Static Routes      :
  To                   Next Hop
  138.203.0.0/16      xxx.xxx.xx.xxx
  172.0.0.0/8         xxx.xxx.xx.xxx
ICMP Vendor Enhancement: Disabled
ATM Location ID        : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ATM OAM Retry Up       : 2
ATM OAM Retry Down     : 4
ATM OAM Loopback Period: 10
=====
A:Dut-F#

```

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.
Parameters	neighbor — Displays LLDP neighbor information.
Output	

Sample Output

```

*A:Dut-C# show system lldp neighbor
Link Layer Discovery Protocol (LLDP) System Information
=====
NB = nearest-bridge   NTMPR = nearest-non-tpmr   NC = nearest-customer
=====
Port      Scope  Chassis ID                Index  Port ID    System Name
-----
1/1/1     NB     16:2f:ff:00:00:00         1      35717120   Dut-A
2/1/2     NB     16:34:ff:00:00:00         1      35782656   Dut-D
2/1/1     NB     16:36:ff:00:00:00         2      35684352   Dut-E
1/1/2     NB     16:30:ff:00:00:00         2      35749888   Dut-B
1/1/3     NB     16:30:ff:00:00:00         3      35782656   Dut-B
2/1/3     NB     16:30:ff:00:00:00         3      35815424   Dut-B
=====

```

```
Number of neighbors : 6
*A:Dut-C#
```

```
A:GHR-API# show system lldp neighbor
Link Layer Discovery Protocol (LLDP) System Information
=====
NB = nearest-bridge   NTMPR = nearest-non-tpmr   NC = nearest-customer
=====
Port      Scope  Chassis ID          Index  Port ID  System Name
-----
1/1/6     NTPMR  00:21:05:1b:bc:17   1      36044800  RXI-AMI
1/1/8     NTPMR  00:21:06:6d:bd:53   2      36110336  YOY-WOW
1/1/9     NTPMR  00:21:08:2b:ab:81   3      36143104  FRI-MON
=====
Number of neighbors : 3
```

load-balancing-alg

Syntax **load-balancing-alg [detail]**

Context show>system

Description This command displays system load balancing settings.

Parameters **detail** — Displays port settings.

Output

Sample Output

```
*A:ALA-49>show>system# load-balancing-alg
=====
System-wide Load Balancing Algorithms
=====
L4   - Load Balance           : exclude-L4
LSR  - Load Balance           : lbl-only
=====
*A:ALA-49>show>system#
```

memory-pools

Syntax **memory-pools**

Context show>system

Description This command displays system memory status.

Output The following table describes memory pool output fields.

Table 51 **System Memory-Pools 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.

Sample Output

A:ALA-1# show system memory-pools

```

=====
Memory Pools
=====
Name                Max Allowed    Current Size    Max So Far      In Use
-----
System              No limit      24,117,248     24,117,248     16,974,832
Icc                 8,388,608     1,048,576     1,048,576       85,200
RTM/Policies       No limit      5,242,912     5,242,912     3,944,104
OSPF               No limit      3,145,728     3,145,728     2,617,384
MPLS/RSVP         No limit      9,769,480     9,769,480     8,173,760
LDP                No limit           0           0           0
IS-IS              No limit           0           0           0
RIP                No limit           0           0           0
VRRP               No limit      1,048,576     1,048,576        96
BGP                No limit      2,097,152     2,097,152     1,624,800
BGP                No limit      2,097,152     2,097,152     1,624,800
Services           No limit      2,097,152     2,097,152     1,589,824
IOM                No limit     205,226,800    205,226,800    202,962,744
SIM                No limit      1,048,576     1,048,576        392
CFLOWD             No limit           0     1,048,576         0
CFLOWD             No limit           0     1,048,576         0
IGMP               No limit           0           0           0
PIM                No limit           0           0           0
ATM                No limit      2,872,648     2,872,648     2,790,104
PIM                No limit           0           0           0
MMPI               No limit           0           0           0
MFIB               No limit           0           0           0
PIP                No limit      79,943,024     79,943,024     78,895,248
MBUF               67,108,864     5,837,328     5,837,328     4,834,280
-----
Current Total Size :    343,495,200 bytes
Total In Use       :    324,492,768 bytes

```

```

Available Memory      :      640,178,652 bytes
=====
A:ALA-1#

```

ntp**Syntax** **ntp****Context** show>system**Description** This command displays NTP protocol configuration and state.**Output** The following table describes NTP output fields.**Table 52** **Show NTP Field Description**

Label	Description
Enabled	yes — NTP is enabled.
	no — NTP is disabled.
Admin Status	yes — Administrative state is enabled.
	no — Administrative state is disabled.
NTP Server	Displays NTP server state of this node.
Stratum	Displays stratum level of this node.
Oper Status	yes — The operational state is enabled.
	no — The operational state is disabled.
Auth Check	Displays the authentication requirement
System Ref. ID	IP address of this node or a 4-character ASCII code showing the state.
Auth Error	Displays the number of authentication errors.
Auth Errors Ignored	Displays the number of authentication errors ignored.
Auth key ID Errors	Displays the number of key identification errors.
Auth Key Type Errors	Displays the number of authentication key type errors.
Reject	The peer is rejected and will not be used for synchronization. Rejection reasons could be the peer is unreachable, the peer is synchronized to this local server so synchronizing with it would create a sync loop, or the synchronization distance is too large. This is the normal startup state.

Table 52 Show NTP Field Description (Continued)

Label	Description (Continued)
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 ten other peers. This peer will not be used for synchronization.
Outlier	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	<p>When stratum is between 0 and 15 this field shows the IP address of the remote NTP server or peer with which the remote 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 displays the following codes:</p> <p>Peer Codes:</p> <p>ACST — The association belongs to any cast server.</p> <p>AUTH — Server authentication failed. Please wait while the association is restarted.</p> <p>AUTO — Autokey sequence failed. Please wait while the association is restarted.</p> <p>BCST — The association belongs to a broadcast server.</p> <p>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.</p> <p>DENY — Access denied by remote server. No further messages will be sent to the server.</p>

Table 52 Show NTP Field Description (Continued)

Label	Description (Continued)
Reference ID (cont.)	<p>DROP — Lost peer in symmetric mode. Please wait while the association is restarted.</p> <p>RSTR — Access denied due to local policy. No further messages will be sent to the server.</p> <p>INIT — The association has not yet synchronized for the first time.</p> <p>MCST — The association belongs to a manycast server.</p> <p>NKEY — No key found. Either the key was never installed or is not trusted.</p> <p>RATE — Rate exceeded. The server has temporarily denied access because the client exceeded the rate threshold.</p> <p>RMOT — The association from a remote host running ntpdc has had unauthorized attempted access.</p> <p>STEP — A step change in system time has occurred, but the association has not yet resynchronized.</p> <p>System Codes</p> <p>INIT — The system clock has not yet synchronized for the first time.</p> <p>STEP — A step change in system time has occurred, but the system clock has not yet resynchronized.</p>
St	Stratum level of this node.
Auth	yes — Authentication is enabled.
	no — Authentication is disabled.
Poll	Polling interval in seconds.
R	Yes — The NTP peer or server has been reached at least once in the last 8 polls.
	No — The NTP peer or server has not been reached at least once in the last 8 polls.
Offset	The time between the local and remote UTC time, in milliseconds.

Sample Output

```

*A:Dut-A# show system ntp
=====
NTP Status
=====
Configured      : Yes           Stratum         : 4
Admin Status   : up            Oper Status     : up
Server Enabled  : No           Server Authenticate : No
Clock Source    : 1111:2222:3333:4444:5555:10:100:2
Auth Check      : Yes
Current Date & Time: 2015/07/10 12:46:30 UTC

```

```

=====
*A:Dut-A# show system ntp all
=====
NTP Status
=====
Configured      : Yes          Stratum          : 4
Admin Status    : up           Oper Status      : up
Server Enabled  : No           Server Authenticate : No
Clock Source     : 1111:2222:3333:4444:5555:10:100:2
Auth Check      : Yes
Current Date & Time: 2015/07/10 12:46:32 UTC
=====

NTP Active Associations
=====
State           Reference ID   St Type  A  Poll Reach      Offset (ms)
  Remote
-----
candidate       252.242.213.211 3  srvr  -  64  YYYYYYYY -5.829
  10.10.1.2
candidate       252.242.213.211 3  srvr  -  64  YYYYYYYY -6.889
  10.10.100.2
chosen          252.242.213.211 3  srvr  -  64  ...YYYYY -6.804
  1111:2222:3333:4444:5555:10:100:2
=====

NTP Clients
=====
vRouter                                     Time Last Request Rx
  Address
-----

*A:Dut-A# show system ntp detail
=====
NTP Status
=====
Configured      : Yes          Stratum          : 4
Admin Status    : up           Oper Status      : up
Server Enabled  : No           Server Authenticate : No
Clock Source     : 1111:2222:3333:4444:5555:10:100:2
Auth Check      : Yes
Auth Errors      : 0           Auth Errors Ignored : 0
Auth Key Id Errors : 0         Auth Key Type Errors : 0
Current Date & Time: 2015/07/10 12:46:34 UTC
=====

NTP Configured Broadcast/Multicast Interfaces
=====
vRouter          Interface      Address          Type    Auth    Poll
-----
=====

*A:Dut-A# show system ntp detail all
=====
NTP Status
=====
Configured      : Yes          Stratum          : 4

```

```

Admin Status      : up                Oper Status      : up
Server Enabled    : No                Server Authenticate : No
Clock Source      : 1111:2222:3333:4444:5555:10:100:2
Auth Check        : Yes
Auth Errors       : 0                Auth Errors Ignored : 0
Auth Key Id Errors : 0                Auth Key Type Errors : 0
Current Date & Time: 2015/07/10 12:46:36 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
-----
candidate      252.242.213.211 3  srvr  -  64  YYYYYYYY -5.829
  10.10.1.2
candidate      252.242.213.211 3  srvr  -  64  YYYYYYYY -6.889
  10.10.100.2
chosen         252.242.213.211 3  srvr  -  64  ...YYYYY -6.804
  1111:2222:3333:4444:5555:10:100:2
=====
NTP Clients
=====
vRouter      Time Last Request Rx
Address
-----
=====
*A:Dut-A#

```

OES

Syntax	oes
Context	show>system
Description	This command displays Optical Extension Shelf (OES) configuration and state information.
Output	The following table describes OES show output.

Table 53 **System Show OES Field Descriptions**

Label	Description
Control Process Status	An overall indication of the state of the OES unprovisioned—The OES chassis is not provisioned. discovering—OES discovery is in progress. active—The OES is ready for operation. inactive—Communication is down; OES not responding. provInProgress—A configuration has been issued to the OES but it has not yet completed.
NTP status	The status of the NTP unknown—Communication with the OES is down. freerun—The OES has never had NTP sync and the router host is not responding to requests. holdover—The OES had NTP sync but has lost communication with the router host. sync—The OES is synchronizing to the router host.
Control Communications	The control communication information between the router and the OES chassis.
Status	The status of the Control Communications. Up—Control communications are up between the router and the OES chassis. Down—Control communications are down between the router and the OES chassis.

Table 53 **System Show OES Field Descriptions (Continued)**

Label	Description
Reason Down	<p>The reason why control communications are down between the router and the OES chassis.</p> <p>Unknown—unknown reason</p> <p>adminReboot—The host initiated a reboot of the OES.</p> <p>heartbeatFailure—The OES did not respond to a heartbeat communication.</p> <p>noResponse—The OES did not respond to a request from the host.</p> <p>configFailed—Either the OES rejected the configuration request (due to software incompatibility) or a timeout occurred while waiting for the MIB set request.</p> <p>invalidSystem—The software on the OES is not reporting the expected sysObjectId.</p> <p>invalidSoftware—The software on the OES is not a compatible release for the router host.</p> <p>mibwalkFailed—A timeout occurred while waiting for a response during mibwalk.</p> <p>oesUnreachable—R14 is only based on a VRF reachability status indication.</p> <p>adminECSwitchover—The host initiated an EC switchover on the OES.</p> <p>ctlCommsUnprov—Control communications have been deprovisioned and there was an outstanding error condition.</p>
OES Software Upgrade	OES software upgrade information
Upgrade Status	The upgrade status; either None, in Progress, Paused, Failed, or Successful.
Cancel Status	The upgrade cancel status; either None, in Progress, Paused, Failed, or Successful.
Software Repository	The software repository name.
Last Upgrade Initiated Time	The last time the upgrade was initiated.
Last Upgrade Completion Time	The time it took to complete the last upgrade.
Last Upgrade Initiated User	The user who initiated the last upgrade.

Sample Output

```

A:bkvm21# show system oes
=====
OES Information
=====
CF Cache Location           : cfl
Running S/W Image           : 1830PSS-8.0-2

```



```
Control Process Status      : OES Control Process status below
NTP status                  : unknown | freerun | holdover | sync
Control Communications
  Status                    : Up | Down
  Reason Down               : Control Comms Down Reason below
OES Software Upgrade
  Upgrade Status            : None | in Progress | Paused | Failed | Successful
  Cancel Status             : None | in Progress | Paused | Failed | Successful
  Software Repository       : <repository name>
  Last Upgrade Initiated Time : None or 2015/01/12 17:57:32 UTC
  Last Upgrade Completion Time : None or 2015/01/12 18:42:11 UTC
  Last Upgrade Initiated User  : N/A
```

port-topology

Syntax	port-topology [uni-dir]
Context	show>system
Description	This command generates a listing of the internal connections within the router. These include connections to satellites and OES ports. Use of the uni-dir keyword will list each connection twice; once for each direction.
Parameters	uni-dir — specifies to list each direction as a separate row
Output	

Sample Output

```
*A:bkvm20# show system port-topology
=====
Port Topology
=====
Port          Far-end
Id            Port Id
-----
1/1/5         oes-1/12/c5
1/1/6         oes-1/12/c9
1/1/20        oes-1/12/c1
-----
No. of Number of port-topology associations: 3
=====
*A:bkvm20# show system port-topology uni-dir
=====
Port Topology
=====
Port          Far-end
Id            Port Id
-----
1/1/5         oes-1/12/c5
oes-1/12/c5   1/1/5
1/1/6         oes-1/12/c9
oes-1/12/c9   1/1/6
1/1/20        oes-1/12/c1
```

```

oes-1/12/c1      1/1/20
-----
No. of Number of port-topology associations: 3
=====

*A:Dut-A# show system port-topology

=====
Port Topology
=====
Port          Far-end
Id            Port Id
-----
esat-1/1/u1    1/1/1
esat-1/1/u2    1/1/2
esat-1/1/u3    1/2/1
esat-1/1/u4    1/2/2
esat-20/1/u1   1/1/3
esat-20/1/u2   1/2/3
esat-20/1/u3   2/1/3
esat-20/1/u4   2/2/3
-----
No. of Number of port-topology associations: 8
=====

```

ptp

Syntax	ptp [standby] ptp peers [router router-instance service-name service-name] [detail] ptp port ptp port port-id [detail] ptp statistics ptp unicast [router router-instance service-name service-name]
Context	show>system
Description	These commands display Precision Time Protocol (PTP) configuration and state information. This information can be displayed for the entire node or on a per router instance basis.
Parameters	standby — Displays information for PTP on the standby control module. unicast — Displays information related to the unicast sessions. statistics — Displays the message and error statistics for the node. peers — Displays summary information for the PTP peers. peer — Displays information for a single PTP peer. router router-instance — Qualifier to show only the information for a specific router instance. detail — Provides additional information on the specified area.

router-instance — *router-name* | *service-id*

Values *router-name* - Base

Values *service-id* - [1 to 2147483647]

Output The following table describes PTP output fields.

Table 54 System PTP Field Descriptions

Label	Description
Pending	When the SR/ESS has initiated a request to a peer but has not yet received a response.
Granted	When the SR/ESS has initiated a request to a peer and it was granted OR a peer has made a request of the SR/ESS and it was granted.
Denied	When the SR/ESS has initiated a request to a peer but it was rejected.
Canceled	When a cancel message has been received from or transmitted toward a peer.
Expired	When a unicast session between the SR/ESS and the peer has expired without being renewed.

Sample Output

```

B: NS082761964# show system ptp
=====
IEEE 1588/PTP Clock Information
=====
-----
Local Clock
-----
Clock Type       : boundary      PTP Profile      : ITU-T G.8275.1
Domain          : 0              Network Type     : sdh
Admin State     : up             Oper State       : up
Announce Interval : 1 pkt/2 s    Announce Rx Timeout : 3 intervals
Peer Limit      : none (Base Router) G.8275.1 Priority : 128
Clock Id        : 001af0fffeb2fead Clock Class      : 255 (slave-only)
Clock Accuracy   : 0xfe (unknown) Clock Variance    : ffff (not computed)
Clock Priority1  : 128            Clock Priority2   : 128
PTP Recovery State: locked       Last Changed     : 08/24/2010 13:17:37
Frequency Offset : +231.920 ppb
-----
Parent Clock
-----
IP Address       : 2.1.1.1        Router           : Base
Port             : 1/2/8         Remote MAC Address: 01:02:03:04:05:06
Local Clock is Parent Clock
Parent Clock Id  : 001af0fffeb36ad Parent Port Number: 2
GM Clock Id     : 00b0aeffffe011ca6 GM Clock Class   : 13
GM Clock Accuracy : 0xfe (unknown) GM Clock Variance : 0x6400 (3.7E-09)
GM Clock Priority1: 128           GM Clock Priority2: 128
-----

```

Time Information

```
-----
Timescale           : PTP
Current Time        : 2011-08-30 15:31:42.99 UTC
Frequency Traceable : yes
Time Traceable      : yes
Time Source         : gps
=====
```

```
B:NS082761964# show system ptp standby
```

IEEE 1588/PTP Clock Information

Local Clock

```
-----
Clock Type          : ordinary,slave      PTP Profile         : ieee1588-2008
Domain              : 0
Admin State         : up                  Oper State          : up
Announce Interval   : 1 pkt/2 s          Announce Rx Timeout : 3 intervals
Clock Id            : 001af0ffffeb2fead   Clock Class         : 255 (slave-only)
Clock Accuracy       : 0xfe (unknown)      Clock Variance      : ffff (not computed)
Clock Priority1      : 128                 Clock Priority2      : 128
PTP Port State      : listening            Last Changed        : 02/11/2013 18:09:58
PTP Recovery State   : locked              Last Changed        : 08/24/2010 13:17:37
Frequency Offset     : +231.920 ppb
=====
```

Parent Clock

```
-----
IP Address          : 2.1.1.1
Parent Clock Id     : 001af0ffffeab36ad   Remote PTP Port Number: 2
GM Clock Id         : 00b0aeffffe011ca6   GM Clock Class       : 13
GM Clock Accuracy   : 0xfe (unknown)      GM Clock Variance    : 0x6400 (3.7E-09)
GM Clock Priority1   : 128                 GM Clock Priority2    : 128
=====
```

Time Information

```
-----
Timescale           : PTP
Current Time        : 2011-08-30 15:31:42.99 UTC
Frequency Traceable : yes
Time Traceable      : yes
Time Source         : gps
=====
```

```
A:bksim1619# show system ptp statistics
```

IEEE 1588/PTP Packet Statistics

```
=====
                                     Input      Output
-----
PTP Packets                        2910253      2393354
  Announce                          9015         22682
  Sync                            1153275      622585
  Follow Up                          0             0
  Delay Request                     594036      1153568
  Delay Response                    1153044      593614
  Signaling                          883          905
=====
```

Request TLVs	428	598		
Announce	304	350		
Sync	62	124		
Delay Response	62	124		
Grant TLVs (Granted)	514	428		
Announce	272	304		
Sync	121	62		
Delay Response	121	62		
Grant TLVs (Rejected)	0	0		
Announce	0	0		
Sync	0	0		
Delay Response	0	0		
Cancel TLVs	3	0		
Announce	1	0		
Sync	1	0		
Delay Response	1	0		
Ack Cancel TLVs	0	3		
Announce	0	1		
Sync	0	1		
Delay Response	0	1		
Other TLVs	0	0		
Other	0	0		
Event Packets timestamped at port	215523	215371		
Event Packets timestamped in software	0	0		
Discards	0	0		
Bad domain value	0	0		
Alternate Master Flag Set	0	0		
Other	0	0		
=====				
IEEE 1588/PTP Clock Recovery State Statistics				
=====				
State	Seconds			

Initial	136			
Acquiring	0			
Phase-Tracking	0			
Locked	0			
Hold-over	0			
=====				
IEEE 1588/PTP Clock Recovery Event Statistics				
=====				
Event	Count			

Packet Loss	0			
Excessive Packet Loss	0			
Excessive Phase Shift Detected	0			
Too Much Packet Delay Variation	0			
=====				
IEEE 1588/PTP Message Rates Per Second				
=====				
Packet Type	UDP/IP		Ethernet	
	Input	Output	Input	Output

Announce	0	0	16	0
Sync	0	0	32	0

Follow Up	0	0	32	0
Delay Request	0	0	0	4
Delay Response	0	0	4	0
Other	0	0	0	0

Total	0	0	84	4
=====				
=====				

```
*A:bksim1618# show system ptp peers
```

```
=====
```

```
IEEE 1588/PTP Peer Information
```

```
=====
```

```
Router
```

	IP Address	Anno Flow	Admin State	PTP Port	State	Parent	Clock

Base							
1	1.4.1.21	tx	n/a	master		no	
	1.2.1.20	rx+tx	up	master		no	
	1.3.1.19	rx	up	slave		yes	
2	1.1.1.21	tx	n/a	master		no	

```
-----
```

```
No. of PTP Peers: 4
```

```
=====
```

```
*A:bksim1618# show system ptp peers router Base
```

```
=====
```

```
IEEE 1588/PTP Peer Information
```

```
=====
```

```
Router
```

	IP Address	Anno Flow	Admin State	PTP Port	State	Parent	Clock

Base							
	1.4.1.21	tx	n/a	master		no	

```
-----
```

```
No. of PTP Peers: 1
```

```
=====
```

```
*A:bksim1618# show system ptp peers router 1
```

```
=====
```

```
IEEE 1588/PTP Peer Information
```

```
=====
```

```
Router
```

	IP Address	Anno Flow	Admin State	PTP Port	State	Parent	Clock

1	1.2.1.20	rx+tx	up	master		no	
	1.3.1.19	rx	up	slave		yes	

```
-----
```

```
No. of PTP Peers: 2
```

```
=====
```

```
*A:bksim1618# show system ptp peers detail
```

```
=====
IEEE 1588/PTP Peer Information
=====
Router      : Base
IP Address   : 1.4.1.21      Announce Direction : tx
Admin State  : n/a          G.8275.1 Priority   : 128
Local PTP Port : 3          PTP Port State    : master
Clock Id     : ac65fffffe000000 Remote PTP Port    : 1
-----
Router      : 1
IP Address   : 1.2.1.20      Announce Direction : rx+tx
Admin State  : up           G.8275.1 Priority   : 128
Local PTP Port : 2          PTP Port State    : master
Clock Id     : ac5effffffe000000 Remote PTP Port    : 1
Locked Out   : no           Time Remaining     : n/a
-----
Router      : 1
IP Address   : 1.3.1.19      Announce Direction : rx
Admin State  : up           G.8275.1 Priority   : 128
Local PTP Port : 1          PTP Port State    : slave
Clock Id     : ac5dfffffe000000 Remote PTP Port    : 1
GM Clock Id  : ac5dfffffe000000 GM Clock Class     : 13
GM Clock Accuracy : unknown   GM Clock Variance  : ffff (not computed)
GM Clock Priority1: 0         GM Clock Priority2 : 128
Steps Removed : 0            Parent Clock       : yes
Locked Out    : no           Time Remaining     : n/a
-----
Router      : 2
IP Address   : 1.1.1.21      Announce Direction : tx
Admin State  : n/a          G.8275.1 Priority   : 128
Local PTP Port : 4          PTP Port State    : master
Clock Id     : ac65fffffe000000 Remote PTP Port    : 1
=====
```

*A:bksim1618# show system ptp peers router 1 detail

```
=====
IEEE 1588/PTP Peer Information
=====
Router      : 1
IP Address   : 1.2.1.20      Announce Direction : rx+tx
Admin State  : up           G.8275.1 Priority   : 128
Local PTP Port : 2          PTP Port State    : master
Clock Id     : ac5effffffe000000 Remote PTP Port    : 1
-----
Router      : 1
IP Address   : 1.3.1.19      Announce Direction : rx
Admin State  : up           G.8275.1 Priority   : 128
Local PTP Port : 1          PTP Port State    : slave
Clock Id     : ac5dfffffe000000 Remote PTP Port    : 1
GM Clock Id  : ac5dfffffe000000 GM Clock Class     : 13
GM Clock Accuracy : unknown   GM Clock Variance  : ffff (not computed)
GM Clock Priority1: 0         GM Clock Priority2 : 128
Steps Removed : 0            Parent Clock       : yes
=====
```

A:bksim1620# show system ptp peer 6.1.1.2 router 5

```
=====
```

IEEE 1588/PTP Peer Information

```

=====
Router           : 5
IP Address       : 6.1.1.2           Announce Direction : rx+tx
Admin State     : up                 G.8275.1 Priority   : 128
Local PTP Port   : 2                 PTP Port State     : passive
Clock Id        : ac5dfffffe000000 Remote PTP Port    : 2
GM Clock Id     : ac5cfffffe000000 GM Clock Class     : 13
GM Clock Accuracy : 0xfe (unknown)  GM Clock Variance  : ffff (not computed)
GM Clock Priority1: 128              GM Clock Priority2  : 128
Steps Removed   : 1                 Parent Clock       : no
=====

```

```

A:bksim1620# show system ptp peer 6.1.1.2 router 5 detail
=====

```

IEEE 1588/PTP Peer Information

```

=====
Router Instance  : 5
IP Address       : 6.1.1.2           Announce Direction : rx+tx
Admin State     : up                 G.8275.1 Priority   : 128
Local PTP Port   : 2                 PTP Port State     : passive
Clock Id        : ac5dfffffe000000 Remote PTP Port    : 2
GM Clock Id     : ac5cfffffe000000 GM Clock Class     : 13
GM Clock Accuracy : 0xfe (unknown)  GM Clock Variance  : ffff (not computed)
GM Clock Priority1: 128              GM Clock Priority2  : 128
Steps Removed   : 1                 Parent Clock       : no
=====

```

IEEE 1588/PTP Unicast Negotiation Information

```

=====
IP Address      Dir Type      Rate      Duration State      Time
-----
6.1.1.2         Rx  Announce    1 pkt/2 s  300      Granted  09/01/2010 17:23:04
6.1.1.2         Tx  Announce    1 pkt/2 s  300      Granted  09/01/2010 17:23:04
=====

```

IEEE 1588/PTP Packet Statistics

```

=====
Input      Output
-----
PTP Packets      253      11
Announce         243       1
Sync              0       0
Follow Up        0       0
Delay Request     0       0
Delay Response    0       0
Signaling        10      10
  Request TLVs    6       4
    Announce      6       4
    Sync           0       0
    Delay Response 0       0
  Grant TLVs (Granted) 4       6
    Announce      4       6
    Sync           0       0
    Delay Response 0       0
  Grant TLVs (Rejected) 0       0
    Announce      0       0
    Sync           0       0
=====

```



```

        Delay Response                0          0
        Cancel TLVs                   0          0
        Announce                      0          0
        Sync                          0          0
        Delay Response                0          0
        Ack Cancel TLVs               0          0
        Announce                      0          0
        Sync                          0          0
        Delay Response                0          0
        Other TLVs                    0          0
        Other                         0          0
Discards                             0          0
        Bad PTP domain                0          0
        Alternate Master               0          0
        Out Of Sequence               0          0
        Peer Disabled                  0          0
        Other                         0          0
=====

```

A:bksim1618# show system ptp port 1/1/1 detail

=====

IEEE 1588/PTP Ethernet Port Information

=====

```

Port                : 1/1/2
PTP Admin State     : up                      PTP Oper State      : up
Local MAC Addr      : 02:43:BA:01:00:03      Multicast MAC Addr   : 01:1b:19:00:00:00
G.8275.1 notSlave   : false                  G.8275.1 Priority    : 128
PTP Port Number     : 3                      PTP Port State       : Slave
Cfg Anno Rate       : 1 pkt/2 s              Cfg Sync/Dly Rate    : 64 pkt/s
Neighbor Clocks     : 4                      Timestamp Point       : port
=====

```

A:bksim1618# show system ptp port 1/1/2 detail

=====

IEEE 1588/PTP Ethernet Port Information

=====

```

Port                : 1/1/2
PTP Admin State     : up                      PTP Oper State      : up
Local MAC Addr      : a0:f3:e4:33:ee:a3      Multicast MAC Addr   : 01:1b:19:00:00:00
PTP Port Number     : 1                      PTP Port State       : slave
Cfg Anno Rate       : 1 pkt/2 s              Cfg Sync/Delay Rate  : 64 pkt/s
Neighbors           : 1                      Timestamp Point       : cpm
=====

```

=====

IEEE 1588/PTP Ethernet Port Neighbor Clocks

=====

MAC Address	Clock Id	Port #	Rx Packet Rate
8c:90:d3:c4:3d:f9	a0f3e4fffe637e30	1	128
8c:90:d3:c4:3d:fa	a0f3e4fffe637e30	2	64

No. of Neighbor Clocks: 2

=====

=====

IEEE 1588/PTP Ethernet Port Packet Statistics

```
=====
```

	Input	Output
PTP Packets	3584	1785
Announce	14	0
Sync	1785	0
Follow Up	0	0
Delay Request	0	1785
Delay Response	1785	0
Signaling	0	0
Other	0	0
Discards	0	0
Bad PTP domain	0	0
Alternate Master	0	0
Out Of Sequence	0	0
Other	0	0

```
=====
```

IEEE 1588/PTP Ethernet Port Neighbor Clocks

```
=====
```

MAC Address	Clock Id	Port Num	Rx Packet Rate
01:02:03:04:05:06	ac65fffffe000001	65535	64
01:02:03:04:05:07	ac65fffffe000002	1	0
01:02:03:04:05:08	ac65fffffe000003	2	64
01:02:03:04:05:09	ac65fffffe000004	99	0

```
=====
```

IEEE 1588/PTP Ethernet Port Packet Statistics

```
=====
```

	Input	Output
PTP Packets	253	11
Announce	243	1
Sync	0	0
Follow Up	0	0
Delay Request	0	0
Delay Response	0	0
Signaling	10	10
Other	0	0
Discards	0	0
Bad PTP domain	0	0
Alternate Master	0	0
Out Of Sequence	0	0
Other	0	0

```
=====
```

A:bksim1618# show system ptp port

IEEE 1588/PTP Ethernet Port Summary Information

```
=====
```

Port	PTP Adm/Opr	PTP State	Neighbors	Tx Rate	Rx Rate
10/2/16	up/up	passive	5	12312	4400
1/1/1	up/up	slave	1	12312	4400
1/1/2	up/up	master	61	12312	4400

```
=====
```

```

1/1/3      up/down      disabled      0          0          0
1/1/4      up/up        listening     0          0          0
-----
No. of PTP Ports : 5                      Total  99999      999999

```

*A:bksim1618# show system ptp unicast

=====

IEEE 1588/PTP Unicast Negotiation Information

=====

Router

IP Address	Dir	Type	Rate	Duration	State	Time

Base						
1.4.1.21	Tx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:14:09
1						
1.2.1.20	Rx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:14:19
1.2.1.20	Tx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:13:25
1.2.1.20	Tx	Sync	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.2.1.20	Rx	DelayReq	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.2.1.20	Tx	DelayRsp	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.3.1.19	Rx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:13:16
1.3.1.19	Rx	Sync	64 pkt/s	300	Granted	04/21/2013 19:13:21
1.3.1.19	Tx	DelayReq	64 pkt/s	300	Granted	04/21/2013 19:13:21
1.3.1.19	Rx	DelayRsp	64 pkt/s	300	Granted	04/21/2013 19:13:21
2						
1.1.1.21	Tx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:14:08
1.1.1.21	Tx	Sync	64 pkt/s	300	Granted	04/21/2013 19:14:15
1.1.1.21	Rx	DelayReq	64 pkt/s	300	Granted	04/21/2013 19:14:15
1.1.1.21	Tx	DelayRsp	64 pkt/s	300	Granted	04/21/2013 19:14:15

PTP Peers : 4

Total Packet Rate : 578 packets/second

=====

*A:bksim1618#

A:bksim1618# show system ptp router 1 unicast

=====

IEEE 1588/PTP Unicast Negotiation Information

=====

Router

IP Address	Dir	Type	Rate	Duration	State	Time

1						
1.2.1.20	Rx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:14:19
1.2.1.20	Tx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:13:25
1.2.1.20	Tx	Sync	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.2.1.20	Rx	DelayReq	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.2.1.20	Tx	DelayRsp	64 pkt/s	300	Granted	04/21/2013 19:13:30
1.3.1.19	Rx	Announce	1 pkt/2 s	300	Granted	04/21/2013 19:13:16
1.3.1.19	Rx	Sync	64 pkt/s	300	Granted	04/21/2013 19:13:21
1.3.1.19	Tx	DelayReq	64 pkt/s	300	Granted	04/21/2013 19:13:21
1.3.1.19	Rx	DelayRsp	64 pkt/s	300	Granted	04/21/2013 19:13:21

PTP Peers : 2

Total Packet Rate : 385 packets/second

=====

*A:bksim1618#

rollback

Syntax	rollback
Context	show>system
Description	This command displays rollback configuration and state.
Output	

Sample Output

```

A:dut-a_a># show system rollback
=====
Rollback Information
=====
Rollback Location           : cf1:/Rollback
Save
  Last Rollback Save Result   : In Progress, Successful or Failed
  Last Save Completion Time   : 10/15/2010 21:24:06
Revert
  In Progress                 : Yes, No
  Last Revert Initiated Time  : 10/15/2010 21:26:23
  Last Revert Initiated User  : xyz
  Last Initiated Checkpoint   : cf1:/Rollback.rb.3
  Last Completed Revert Result : Successful or Failed
  Last Revert Completion Time : 10/15/2010 21:27:19
=====
Rollback Files
=====
Idx      Suffix  Creation time      Release  User
      Comment
-----
latest   .rb      2010/10/15 21:24:02  9.0.R4   fred
          This checkpoint was saved after the 3 VPLS services were created
1        .rb.1   2010/10/15 21:23:58  9.0.R4   John
          John's checkpoint on Sunday
2        .rb.2   2010/10/15 21:23:52  9.0.R4   admin
          A long checkpoint comment that an operator is using to summarize
          various some of the changes that were made.  They may even have so
          much to say that they use the maximum comment size.  Notice that
          words are not chopped.
...
9        .rb.9    2010/10/14 22:00:01  9.0.R4   admin
          VPLS services 1000-2000 created
...
53       .rb.53   2010/10/14 22:10:10  9.0.R4   admin
-----
No. of Rollback Files: 10
=====

```

sntp

Syntax	sntp
---------------	-------------

Context show>system

Description This command displays SNTP protocol configuration and state.

Output The following table describes SNTP output fields.

Table 55 System SNTP Field Descriptions

Label	Description
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.

Sample Output

```
A:ALA-1# show system sntp
=====
SNTP
=====
SNTP Server      Version      Preference      Interval
-----
10.10.20.253      3              Preferred        64
=====
A:ALA-1#
```

thresholds

Syntax thresholds

Context show>system

Description This command displays system monitoring thresholds. The Threshold Events Log table will keep only the last 201 entries.

Output The following table describes system threshold output fields.

Table 56 System Thresholds Field Descriptions

Label	Description
Variable	Displays the variable OID.
Alarm Id	Displays the numerical identifier for the alarm.

Table 56 **System Thresholds Field Descriptions (Continued)**

Label	Description (Continued)
Last Value	Displays the last threshold value.
Rising Event Id	Displays the identifier of the RMON rising event.
Threshold	Displays the identifier of the RMON rising threshold.
Falling Event Id	Displays the identifier of the RMON falling event.
Threshold	Displays the identifier of the RMON falling threshold.
Sample Interval	Displays the polling interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds.
SampleType	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds.
Startup Alarm	Displays the alarm that may be sent when this alarm is first created.
Owner	Displays the owner of this alarm.
Description	Displays the event cause.
Event Id	Displays the identifier of the threshold event.
Last Sent	Displays the date and time the alarm was sent.
Action Type	<p>log — An entry is made in the RMON-MIB log table for each event occurrence.</p> <p>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.</p> <p>both — Both an entry in the RMON-MIB logTable and a TiMOS logger event are generated.</p> <p>none — No action is taken</p>
Owner	Displays the owner of the event.

Sample Output

```

A:bkvm3# show system thresholds
=====
Threshold Alarms
=====
Variable: tmnxCpmFlashUsed.1.10.1
Alarm Id       : 1           Last Value : 3192120
Rising Event Id : 1           Threshold  : 10
Falling Event Id : 0          Threshold  : 0
Sample Interval : 1           SampleType : absolute
Startup Alarm   : either      Owner       : TiMOS CLI

```

```
Variable: tmnxCpmFlashUsed.1.10.2
Alarm Id      : 2          Last Value : 0
Rising Event Id : 2          Threshold : 20
Falling Event Id : 3          Threshold : 30
Sample Interval : 2          SampleType : absolute
Startup Alarm   : either    Owner      : TiMOS CLI
```

```
Variable: tmnxCpmFlashPercentageUsed.1.10.1
Alarm Id      : 3          Last Value : 19
Rising Event Id : 4          Threshold : 30
Falling Event Id : 0          Threshold : 0
Sample Interval : 3          SampleType : absolute
Startup Alarm   : either    Owner      : TiMOS CLI
```

```
Variable: tmnxCpmFlashPercentageUsed.1.10.2
Alarm Id      : 4          Last Value : 0
Rising Event Id : 5          Threshold : 40
Falling Event Id : 6          Threshold : 50
Sample Interval : 4          SampleType : absolute
Startup Alarm   : either    Owner      : TiMOS CLI
```

=====

Threshold Events

=====

Description: TiMOS CLI - cflash capacity alarm rising event
using percentages

```
Event Id      : 1          Last Sent  : 07/23/2015 18:15:46
Action Type    : both      Owner      : TiMOS CLI
```

Description: TiMOS CLI - cflash capacity warning rising event

```
Event Id      : 2          Last Sent  : never
Action Type    : both      Owner      : TiMOS CLI
```

Description: TiMOS CLI - cflash capacity warning falling event

```
Event Id      : 3          Last Sent  : 07/23/2015 18:15:46
Action Type    : both      Owner      : TiMOS CLI
```

Description: TiMOS CLI - cflash capacity warning rising event
using percentages

```
Event Id      : 4          Last Sent  : never
Action Type    : both      Owner      : TiMOS CLI
```

Description: TiMOS CLI - cflash capacity alarm rising event
using percentages

```
Event Id      : 5          Last Sent  : never
Action Type    : both      Owner      : TiMOS CLI
```

Description: TiMOS CLI - cflash capacity alarm falling event
using percentages

```
Event Id      : 6          Last Sent  : 07/23/2015 18:15:46
Action Type    : both      Owner      : TiMOS CLI
```

=====

Threshold Events Log

=====

Description : TiMOS CLI - cflash capacity alarm rising
event using percentages : value=3192120,

```

                                >=10 : alarm-index 1, event-index 1 alarm-
                                variable OID tmnxCpmFlashUsed.1.10.1
Event Id      : 1      Time Sent   : 07/23/2015 18:15:46

Description   : TiMOS CLI - cflash capacity warning falling
                                event : value=0, <=30 : alarm-index 2, event-
                                index 3 alarm-variable OID tmnxCpmFlashUsed.
                                1.10.2
Event Id      : 3      Time Sent   : 07/23/2015 18:15:46

Description   : TiMOS CLI - cflash capacity alarm falling
                                event using percentages : value=0, <=50 :
                                alarm-index 4, event-index 6 alarm-variable
                                OID tmnxCpmFlashPercentageUsed.1.10.2
Event Id      : 6      Time Sent   : 07/23/2015 18:15:46

=====
```

time

- Syntax** **time**
- Context** show>system
- Description** This command displays the system time and zone configuration parameters.
- Output** The following table describes system time output fields.

Table 57 System Time Field Descriptions

Label	Description
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.
Zone	The zone names for the current zone, the non-DST zone, and the DST zone if configured.
Current Time Zone	Indicates the process currently controlling the system time. SNTP, NTP, PTP or NONE.
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 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 Daylight Saving Time.

Table 57 System Time Field Descriptions (Continued)

Label	Description (Continued)
Starts	The date and time Daylight Saving Time begins.
Ends	The date and time Daylight Saving Time ends.

Sample Output

```
A:ALA-1# show system time
=====
Date & Time
=====
Current Date & Time : 2006/05/05 23:03:13    DST Active      : yes
Current Zone       : PDT                    Offset from UTC   : -7:00
-----
Non-DST Zone       : PST                    Offset from UTC   : -8:00
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
=====
A:ALA-1#

A:ALA-1# show system time (with no DST zone configured)
=====
Date & Time
=====
Current Date & Time : 2006/05/12 11:12:05    DST Active      : no
Current Zone       : APA                    Offset from UTC   : -8:00
-----
Non-DST Zone       : APA                    Offset from UTC   : -8:00
Zone Type          : non-standard
-----
No DST zone configured
=====
A:ALA-1#
```

time

Syntax	time
Context	show
Description	<p>This command displays the current day, date, time and time zone.</p> <p>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.</p>
Output	

Sample Output

```
A:ALA-49# show time
Tue Oct 31 12:17:15 GMT 2006
```

redundancy

Syntax	redundancy
Context	show
Description	This command enables the context to show redundancy information.

mgmt-ethernet

Syntax	mgmt-ethernet
Context	show>redundancy
Description	This command shows the management Ethernet port redundancy status. The show router “management” interface command also shows the CPM Ethernet port used by the management interface. If the primary CPM’s port is active, then it shows “A/1” under the Port field,. If the secondary CPM’s port is active, then it shows “B/1 -> A/1”in the Port field.
Output	Show Redundancy Mgmt-Ethernet Output

The following table describes the Redundancy Mgmt-Ethernet fields:

Table 58 Redundancy Mgmt-ethernet Field Descriptions

Label	Description
Admin Status	Enabled — Administrative status is enabled. Disabled — Administratively disabled.
Oper Status	Displays the CPM on which the management Ethernet port is operating.
Revert Time	Displays the revert time.

Sample Output

```
A:SR12# show redundancy mgmt-ethernet

=====
Management Ethernet Redundancy
=====
Admin Status   : Enabled
Oper Status    : Management port operating on active CPM
```

Revert Time : 5 seconds

Show Router "Management" Interface Detail Output

The following is a sample output that shows "A/1" when the primary CPM's Ethernet port is active and "B/1 ->A/1" if the secondary CPM's port is active.

*B:Dut-A# show router "management" interface

```
=====
Interface Table (Router: management)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId
IP-Address          PfxState
-----
management          Up        Up/Up        Network B/1 -> A/1
138.120.186.219/24  n/a
3000::8a78:badb/96  PREFERRED
fe80::221:5ff:fece:df49/64  PREFERRED
-----
Interfaces : 1
=====
```

*B:Dut-A# show router "management" interface detail

```
=====
Interface Table (Router: management)
=====

-----
Interface
-----
If Name      : management
Admin State  : Up
Oper (v4/v6) : Up/Up
Protocols    : None
IP Addr/mask : 138.120.186.219/24
Address Type : Primary
IGP Inhibit  : Disabled
Broadcast Address : Host-ones
HoldUp-Time  : 0
Track Srrp Inst : 0
IPv6 Address : 3000::8a78:badb/96
IPv6 Addr State : PREFERRED
CGA modifier : (Not Specified)
HoldUp-Time  : 0
Track Srrp Inst : 0
Link Lcl Address : fe80::221:5ff:fece:df49/64
Link Lcl State : PREFERRED
-----
Details
-----
Description  : (Not Specified)
If Index     : 1280
Virt. If Index : 1280
Last Oper Chg : 06/16/2015 21:01:07
Global If Index : 16384
Lag Link Map Prof: none
Port Id      : B/1 -> A/1
TOS Marking  : Trusted
If Type      : Network
Egress Filter : none
Ingress Filter : none
Egr IPv6 Flt : none
Ingr IPv6 Flt : none
BGP IP FlowSpec : Disabled
BGP IPv6 FlowSpec: Disabled
SNTP B.Cast   : True
Network QoS Policy: 1
-----
```

MAC Address : 00:21:05:ce:df:49 Mac Accounting : Disabled

multi-chassis

Syntax **multi-chassis**

Context show>redundancy

Description This command enables the context to show multi-chassis redundancy information.

all

Syntax **all [detail]**

Context show>redundancy>multi-chassis

Description This command displays brief multi-chassis redundancy information.

Parameters **detail** — Shows detailed multi-chassis redundancy information.

Output The following table describes Redundancy Multi-Chassis All fields:

Table 59 Redundancy multi-chassis all Field Descriptions

Label	Description
Peer IP Address	Displays the multi-chassis redundancy peer.
Description	The text string describing the peer.
Authentication	If configured, displays the authentication key used between this node and the MC peer.
Source IP Address	Displays the source address used to communicate with the MC peer.
Admin State	Displays the administrative state of the peer.

Sample Output

```
B:Dut-B# show redundancy multi-chassis all
=====
Multi-chassis Peer Table
=====
Peer
-----
Peer IP Address      : 10.10.10.2
Description          : Mc-Lag peer 10.10.10.2
Authentication       : Disabled
Source IP Address    : 0.0.0.0
```

```

Admin State          : Enabled
=====
B:Dut-B#

B:Dut-B# show lag detail
=====
LAG Details
=====
LAG 1
-----
Description: Description For LAG Number 1
-----
Details
-----
Lag-id              : 1                Mode              : access
Adm                  : up                Opr               : up
Thres. Exceeded Cnt : 9                Port Threshold    : 0
Thres. Last Cleared  : 05/20/2006 00:12:35 Threshold Action   : down
Dynamic Cost         : false            Encap Type        : null
Configured Address   : 1c:71:ff:00:01:41 Lag-IfIndex       : 1342177281
Hardware Address     : 1c:71:ff:00:01:41 Adapt Qos        : distribute
Hold-time Down       : 0.0 sec
LACP                 : enabled           Mode              : active
LACP Transmit Intvl  : fast              LACP xmit stdby   : enabled
Selection Criteria   : highest-count      Slave-to-partner   : disabled
Number of sub-groups: 1                  Forced            : -
System Id           : 1c:71:ff:00:00:00 System Priority     : 32768
Admin Key            : 32768              Oper Key           : 32666
Prtr System Id       : 20:f4:ff:00:00:00 Prtr System Priority : 32768
Prtr Oper Key        : 32768

MC Peer Address      : 10.10.10.2         MC Peer Lag-id     : 1
MC System Id         : 00:00:00:33:33:33 MC System Priority  : 32888
MC Admin Key         : 32666              MC Active/Standby  : active
MC Lacp ID in use    : true               MC extended timeout : false
MC Selection Logic    : peer decided
MC Config Mismatch   : no mismatch
-----
Port-id      Adm    Act/Stdbby Opr    Primary  Sub-group  Forced  Prio
-----
331/2/1      up     active   up     yes      1          -      32768
331/2/2      up     active   up     yes      1          -      32768
331/2/3      up     active   up     yes      1          -      32768
331/2/4      up     active   up     yes      1          -      32768
-----
Port-id      Role    Exp  Def  Dist  Col  Syn  Aggr  Timeout  Activity
-----
331/2/1      actor   No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/1      partner No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/2      actor   No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/2      partner No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/3      actor   No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/3      partner No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/4      actor   No   No   Yes  Yes  Yes  Yes  Yes     Yes
331/2/4      partner No   No   Yes  Yes  Yes  Yes  Yes     Yes
=====
B:Dut-B#

```

mc-endpoint

Syntax	mc-endpoint statistics mc-endpoint peer <i>[ip-address]</i> statistics mc-endpoint endpoint <i>[mcep-id]</i> statistics mc-endpoint peer <i>[ip-address]</i>
Context	show>redundancy>multi-chassis
Description	This command displays multi-chassis endpoint information.
Parameters	statistics — Displays the global statistics for the MC endpoint. peer <i>ip-address</i> — Specifies the IP address of multi-chassis end-point peer. endpoint <i>mcep-id</i> — Specifies the multi-chassis endpoint. Values 1 to 4294967295

Output

Sample Output

```
*A:Dut-B# show redundancy multi-chassis mc-endpoint statistics
=====
Multi-Chassis Endpoint Global Statistics
=====
Packets Rx                               : 533
Packets Rx Keepalive                     : 522
Packets Rx Config                         : 3
Packets Rx Peer Config                   : 1
Packets Rx State                         : 7
Packets Dropped Keep-Alive Task          : 7
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 Tlv Invalid MC-Endpoint Id : 0
Packets Dropped MD5                      : 0
Packets Dropped Unknown Peer             : 0
Packets Dropped MC Endpoint No Peer      : 0
Packets Tx                               : 26099
Packets Tx Keepalive                     : 8221
Packets Tx Config                         : 2
Packets Tx Peer Config                   : 17872
Packets Tx State                         : 4
Packets Tx Failed                        : 0
=====
*A:Dut-B#

*A:Dut-B# show redundancy multi-chassis mc-endpoint peer 3.1.1.3 statistics
=====
Multi-Chassis MC-Endpoint Statistics
=====
Peer Addr                               : 3.1.1.3
-----
```

```

Packets Rx                               : 597
Packets Rx Keepalive                     : 586
Packets Rx Config                         : 3
Packets Rx Peer Config                   : 1
Packets Rx State                         : 7
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                               : 636
Packets Tx Keepalive                     : 600
Packets Tx Peer Config                   : 30
Packets Tx Failed                        : 0
Packets Dropped No Peer                  : 0
=====
*A:Dut-B#

*A:Dut-B# show redundancy multi-chassis mc-endpoint endpoint 1 statistics
=====
Multi-Chassis Endpoint Statistics
=====
MC-Endpoint Id 1
=====
Packets Rx Config                       : 3
Packets Rx State                        : 7
Packets Tx Config                       : 2
Packets Tx State                        : 4
Packets Tx Failed                       : 0
=====
Number of Entries 1
=====

```

mc-lag

Syntax **mc-lag** [**lag** *lag-id*]

Context show>redundancy>multi-chassis

Description This command displays multi-chassis LAG information.

Parameters **lag** *lag-id* — Shows information for the specified LAG identifier.

Values 1 to 800

peer

Syntax **peer** *ip-address* [**lag** *lag-id*]

Context show>redundancy>multi-chassis>mc-lag

Description This command enables the context to display mc-lag peer-related redundancy information.

Parameters *ip-address* — Shows peer information about the specified IP address.

lag *lag-id* — Shows information for the specified LAG identifier.

Values 1 to 800

Output The following table describes show redundancy multi-chassis mc-lag peer output fields:

Table 60 Redundancy Multi-chassis MC-Lag Peer Field Descriptions

Label	Description
Last Changed	Displays date and time of the last mc-lag peer.
Admin State	Displays the administrative state of the mc-lag peer.
Oper State	Displays the operation state of the mc-lag peer.
KeepAlive	Displays the length of time to keep alive the mc-lag peer.
Hold On Ngbr Failure	Specifies how many “keepalive” intervals the standby SR will wait for packets from the active node before assuming a redundant-neighbor node failure.

Sample Output

```
A:subscr_mgt# show redundancy multi-chassis mc-lag peer 10.10.10.30
=====
Multi-Chassis MC-Lag Peer 10.10.10.30
=====
Last Changed      : 01/23/2007 18:20:13
Admin State       : Up
Oper State        : Up
KeepAlive         : 10 deci-seconds
Hold On Ngbr Failure : 3
-----
Lag Id Lacp Key Remote Lag Id System Id          Sys Prio Last Changed
-----
1      1      1          00:00:00:00:00:01  1          01/23/2007 18:20:13
2      2      2          00:00:00:00:00:02  2          01/24/2007 08:53:48
-----
Number of LAGs : 2
=====
A:subscr_mgt#
```

```
A:subscr_mgt# show redundancy multi-chassis mc-lag peer 10.10.10.30 lag 1
=====
Multi-Chassis MC-Lag Peer 10.10.10.30
=====
Last Changed      : 01/23/2007 18:20:13
Admin State       : Up
Oper State        : Up
KeepAlive         : 10 deci-seconds
Hold On Ngbr Failure : 3
-----
Lag Id Lacp Key Remote Lag Id System Id          Sys Prio Last Changed
```



```
-----  
1      1      1      00:00:00:00:00:01  1      01/23/2007 18:20:13  
-----  
Number of LAGs : 1  
=====
```

```
A:subscr_mgt#
```

statistics

Syntax **statistics mc-lag** [**peer** *ip-address* [**lag** *lag-id*]]

Context show>redundancy>multi-chassis>mc-lag

Description This command displays multi-chassis statistics.

Parameters **mc-lag** — Displays multi-chassis LAG statistics.

peer *ip-address* — Shows the specified address of the multi-chassis peer.

lag *lag-id* — Shows information for the specified LAG identifier.

Values 1 to 800

Output The following table describes show redundancy multi-chassis mc-lag peer output fields:

Table 61 Redundancy Multi-chassis MC-Lag Peer Statistics Field Descriptions

Label	Description
Packets Rx	Indicates the number of MC-Lag packets received from the peer.
Packets Rx Keepalive	Indicates the number of MC-Lag keepalive packets received from the peer.
Packets Rx Config	Indicates the number of received MC-Lag configured packets from the peer.
Packets Rx Peer Config	Indicates the number of received MC-Lag packets configured by the peer.
Packets Rx State	Indicates the number of MC-Lag “lag” state packets received from the peer.
Packets Dropped State Disabled	Indicates the number of packets that were dropped because the peer was administratively disabled.
Packets Dropped Packets Too Short	Indicates the number of packets that were dropped because the packet was too short.
Packets Dropped Tlv Invalid Size	Indicates the number of packets that were dropped because the packet size was invalid.

Table 61 Redundancy Multi-chassis MC-Lag Peer Statistics Field Descriptions (Continued)

Label	Description (Continued)
Packets Dropped Tlv Invalid LagId	Indicates the number of packets that were dropped because the packet referred to an invalid or non multi-chassis lag.
Packets Dropped Out of Seq	Indicates the number of packets that were dropped because the packet size was out of sequence.
Packets Dropped Unknown Tlv	Indicates the number of packets that were dropped because the packet contained an unknown TLV.
Packets Dropped MD5	Indicates the number of packets that were dropped because the packet failed MD5 authentication.
Packets Tx	Indicates the number of packets transmitted from this system to the peer.
Packets Tx Keepalive	Indicates the number of keepalive packets transmitted from this system to the peer.
Packets Tx Peer Config	Indicates the number of configured packets transmitted from this system to the peer.
Packets Tx Failed	Indicates the number of packets that failed to be transmitted from this system to the peer.

Sample Output

```

A:subscr_mgt# show redundancy multi-chassis mc-lag statistics
=====
Multi-Chassis Statistics
=====
Packets Rx                : 52535
Packets Rx Keepalive      : 52518
Packets Rx Config         : 2
Packets Rx Peer Config    : 4
Packets Rx State          : 6
Packets Dropped KeepaliveTask : 0
Packets Dropped Packet 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 Tlv Invalid LagId : 0
Packets Dropped MD5       : 0
Packets Dropped Unknown Peer : 0
Packets Tx                : 52583
Packets Tx Keepalive      : 52519
Packets Tx Config         : 2
Packets Tx Peer Config    : 54
Packets Tx State          : 8
Packets Tx Failed         : 0
=====

```

```
A:subscr_mgt#

B:Dut-B# show redundancy multi-chassis mc-lag peer 10.10.10.2 statistics
=====
Multi-Chassis Statistics, Peer 10.10.10.2
=====
Packets Rx                               : 231
Packets Rx Keepalive                     : 216
Packets Rx Config                         : 1
Packets Rx Peer Config                   : 2
Packets Rx State                         : 12
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                               : 235
Packets Tx Keepalive                     : 216
Packets Tx Peer Config                   : 3
Packets Tx Failed                        : 0
=====
B:Dut-B#
```

mc-ring

Syntax **mc-ring peer** *ip-address* **statistics**
mc-ring peer *ip-address* [**ring** *sync-tag* [**detail** | **statistics**]]
mc-ring peer *ip-address* **ring** *sync-tag* **ring-node** [*ring-node-name*] [**detail** | **statistics**]]
mc-ring global-statistics

Context show>redundancy>multi-chassis

Description	This command displays multi-chassis ring information.
--------------------	---

Parameters	<i>ip-address</i> — Specifies the address of the multi-chassis peer to display.
	ring <i>sync-tag</i> — Specifies a synchronization tag to be displayed that was used while synchronizing this port with the multi-chassis peer.
	node <i>ring-node-name</i> — Specifies a ring-node name.
	global-statistics — Displays global statistics for the multi-chassis ring.
	detail — Displays detailed peer information for the multi-chassis ring.

Output The following table describes mc-ring peer ip-address ring output fields.

Table 62 Mc-ring peer ip-address Ring Field Descriptions

Label	Description
Sync Tag	Displays the synchronization tag that was used while synchronizing this port with the multi-chassis peer.
Oper State	noPeer — The peer has no corresponding ring configured.
	connected — The in-band control connection with the peer is operational.
	broken — The in-band control connection with the peer has timed out.
	conflict — The in-band control connection with the peer has timed out but the physical connection is still OK; the failure of the in-band signaling connection is caused by a misconfiguration. For example, a conflict between the configuration of this system and its peer, or a misconfiguration on one of the ring access node systems.
	testingRing — The in-band control connection with the peer is being set up. Waiting for result.
	waitingForPeer — Verifying if this ring is configured on the peer.
	configErr — The ring is administratively up, but a configuration error prevents it from operating properly.
	halfBroken — The in-band control connection indicates that the ring is broken in one direction (towards the peer).
	localBroken — The in-band control connection with the peer is known to be broken due to local failure or local administrative action.
Oper state	shutdown — The ring is shutdown.
Failure Reason	Displays the reason of the failure of the operational state of a MC ring.
No. of MC Ring entries	Displays the number of MC ring entries.

Sample Output

```
*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 10.0.0.2 ring ring11 detail
=====
Multi-Chassis MC-Ring Detailed Information
=====
Peer           : 10.0.0.2
Sync Tag       : ring11
Port ID        : 1/1/3
Admin State    : inService
```

```

Oper State      : connected
Admin Change   : 01/07/2008 21:40:07
Oper Change    : 01/07/2008 21:40:24
Failure Reason : None
-----
In Band Control Path
-----
Service ID     : 10
Interface Name : to_an1
Oper State     : connected
Dest IP       : 10.10.0.2
Src IP        : 10.10.0.1
-----
VLAN Map B Path Provisioned
-----
range 13-13
range 17-17
-----
VLAN Map Excluded Path Provisioned
-----
range 18-18
-----
VLAN Map B Path Operational
-----
range 13-13
range 17-17
-----
VLAN Map Excluded Path Operational
-----
range 18-18
=====
*A:ALA-48>show>redundancy>multi-chassis#

*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 192.251.10.104
=====
MC Ring entries
=====
Sync Tag                               Oper State      Failure Reason
-----
No. of MC Ring entries: 0
=====
*A:ALA-48>show>redundancy>multi-chassis#

*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 10.0.0.2
=====
MC Ring entries
=====
Sync Tag                               Oper State      Failure Reason
-----
ring11                                connected       None
ring12                                shutdown        None
-----
No. of MC Ring entries: 4
=====
*A:ALA-48>show>redundancy>multi-chassis#

```

```
*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 10.0.0.2 ring ring11 ring-
node an1 detail
=====
Multi-Chassis MC-Ring Node Detailed Information
=====
Peer          : 10.0.0.2
Sync Tag      : ring11
Node Name     : an1
Oper State Loc : connected
Oper State Rem : notTested
In Use        : True
Admin Change  : 01/07/2008 21:40:07
Oper Change   : 01/07/2008 21:40:25
Failure Reason : None
-----
Ring Node Connectivity Verification
-----
Admin State   : inService
Service ID    : 11
VLAN Tag      : 11
Dest IP       : 10.11.3.1
Src IP        : None
Interval      : 1 minutes
Src MAC       : None
=====
*A:ALA-48>show>redundancy>multi-chassis#

*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 10.0.0.2 ring ring11 ring-node
=====
MC Ring Node entries
=====
Name          Loc Oper St.      Failure Reason
In Use        Rem Oper St.
-----
an1           connected        None
Yes           notTested
an2           connected        None
Yes           notTested
-----
No. of MC Ring Node entries: 2
=====
*A:ALA-48>show>redundancy>multi-chassis#
```

The following table describes multi-chassis ring peer output fields.

Table 63 Redundancy Multi-Chassis Ring Peer Statistics Field Descriptions

Label	Description
Message	Displays the message type.
Received	Indicates the number of valid MC-ring signaling messages received from the peer.

Table 63 Redundancy Multi-Chassis Ring Peer Statistics Field Descriptions (Continued)

Label	Description (Continued)
Transmitted	Indicates the number of valid MC-ring signaling messages transmitted from the peer.
MCS ID Request	Displays the number of valid MCS ID requests were received from the peer.
MCS ID Response	Displays the number of valid MCS ID responses were received from the peer.
Ring Exists Request	Displays the number of valid 'ring exists' requests were received from the peer.
Ring Exists Response	Displays the number of valid ring exists' responses were received from the peer.
Keepalive	Displays the number of valid MC-ring control packets of type 'keepalive' were received from the peer.

Sample Output

```
*A:ALA-48>show>redundancy>multi-chassis# mc-ring peer 192.251.10.104 statistics
=====
MC Ring statistics for peer 192.251.10.104
=====
Message                                     Received      Transmitted
-----
MCS ID Request                             0             0
MCS ID Response                             0             0
Ring Exists Request                         0             0
Ring Exists Response                         0             0
Keepalive                                   0             0
-----
Total                                       0             0
=====
*A:ALA-48>show>redundancy>multi-chassis#
```

Show mc-ring fields

Table 64 Mc-ring ring-node Command Field Descriptions

Label	Description
Oper State	Displays the state of the connection verification (both local and remote).
	notProvisioned — Connection verification is not provisioned.
	configErr — Connection verification is provisioned but a configuration error prevents it from operating properly.
	notTested — Connection verification is administratively disabled or is not possible in the current situation.
	testing — Connection Verification is active, but no results are yet available.
	connected — The ring node is reachable.
	disconnected — Connection verification has timed out.
In Use	Displays “True” if the ring node is referenced on an e-pipe or as an inter-dest-id on a static host or dynamic lease.

Table 65 Mc-ring global-statistics Command Field Descriptions

Label	Description
Rx	Displays the number of MC-ring signaling packets were received by this system.
Rx Too Short	Displays the number of MC-ring signaling packets were received by this system that were too short.
Rx Wrong Authentication	Displays the number of MC-ring signaling packets were received by this system with invalid authentication.
Rx Invalid TLV	Displays the number of MC-ring signaling packets were received by this system with invalid TLV.
Rx Incomplete	Displays the number of MC-ring signaling packets were received by this system that were incomplete.
Rx Unknown Type	Displays the number of MC-ring signaling packets were received by this system that were of unknown type.
Rx Unknown Peer	Displays the number of MC-ring signaling packets were received by this system that were related to an unknown peer.
Rx Unknown Ring	Displays the number of MC-ring signaling packets were received by this system that were related to an unknown ring.

Table 65 Mc-ring global-statistics Command Field Descriptions

Label	Description
Rx Unknown Ring Node	Displays the number of MC-ring signaling packets were received by this system that were related to an unknown ring node.
Tx	Displays the number of MC-ring signaling packets were transmitted by this system.
Tx No Buffer	Displays the number of MC-ring signaling packets could not be transmitted by this system due to a lack of packet buffers.
Tx Transmission Failed	Displays the number of MC-ring signaling packets could not be transmitted by this system due to a transmission failure.
Tx Unknown Destination	Displays the number of MC-ring 'unknown destination' signaling packets were transmitted by this system.
Missed Configuration Events	Displays the number of missed configuration events on this system.
Missed BFD Events	Displays the number of missed BFD events on this system.

```
*A:ALA-48>show>redundancy>multi-chassis# mc-ring global-statistics
=====
Global MC Ring statistics
=====
Rx                                     : 0
Rx Too Short                         : 0
Rx Wrong Authentication              : 0
Rx Invalid TLV                      : 0
Rx Incomplete                       : 0
Rx Unknown Type                     : 0
Rx Unknown Peer                     : 0
Rx Unknown Ring                     : 0
Rx Unknown Ring Node                : 0
Tx                                   : 36763
Tx No Buffer                          : 0
Tx Transmission Failed               : 0
Tx Unknown Destination               : 0
Missed Configuration Events          : 0
Missed BFD Events                    : 0
=====
*A:ALA-48>show>redundancy>multi-chassis#
```

sync

Syntax **sync** [port *port-id* | *lag-id*]

Context show>redundancy>multi-chassis

Description This command displays synchronization information.

Parameters **port** *port-id* — Shows the specified port ID of the multi-chassis peer.

lag *lag-id* — Shows information for the specified LAG identifier.

Values 1 to 800

Output The following table describes show redundancy multi-chassis sync output fields:

Table 66 Redundancy Multi-chassis Sync Field Descriptions

Label	Description
Peer IP Address	Displays the multi-chassis redundancy peer.
Description	The text string describing the peer.
Authentication	If configured, displays the authentication key used between this node and the multi-chassis peer.
Source IP Address	Displays the source address used to communicate with the multi-chassis peer.
Admin State	Displays the administrative state of the peer.
Client Applications	Displays the list of client applications synchronized between SRs.
Sync Admin State	Displays the administrative state of the synchronization.
Sync Oper State	Displays the operation state of the synchronization.
DB Sync State	Displays the database state of the synchronization.
Num Entries	Displays the number of entries on local router.
Lcl Deleted Entries	Displays the number of deleted entries made at the local router.
Alarm Entries	Displays the alarm entries on the local router.
Rem Num Entries	Displays the number of entries on the remote router.
Rem Lcl Deleted Entries	Displays the number of locally deleting entries made by the remote router.
Rem Alarm Entries	Displays alarm entries on the remote router.

Sample Output

```
*A:subscr_mgt_2# show redundancy multi-chassis sync
=====
Multi-chassis Peer Table
=====
Peer
-----
Peer IP Address      : 10.10.10.20
```

```
Description          : Mc-Lag peer 10.10.10.20
Authentication       : Disabled
Source IP Address    : 0.0.0.0
Admin State          : Enabled
-----
Sync-status
-----
Client Applications   : SUBMGMT
Sync Admin State      : Up
Sync Oper State       : Up
DB Sync State         : inSync
Num Entries           : 1
Lcl Deleted Entries   : 0
Alarm Entries         : 0
Rem Num Entries       : 1
Rem Lcl Deleted Entries : 0
Rem Alarm Entries     : 0
=====
A:subscr_mgt_2#
```

peer

Syntax **peer** *ip-address*

Context show>redundancy>multi-chassis>sync

Description This command enables the context to display peer-related redundancy information.

Parameters *ip-address* — Shows peer information about the specified IP address.

Output The following table describes show redundancy multi-chassis sync output fields:

Table 67 Redundancy Multi-chassis Sync Peer Field Descriptions

Label	Description
Peer IP Address	Displays the multi-chassis redundancy peer.
Description	The text string describing the peer.
Authentication	If configured, displays the authentication key used between this node and the multi-chassis peer.
Source IP Address	Displays the source address used to communicate with the multi-chassis peer.
Admin State	Displays the administrative state of the peer.
Client Applications	Displays the list of client applications synchronized between SRs.
Sync Admin State	Displays the administrative state of the synchronization.
Sync Oper State	Displays the operation state of the synchronization.

Table 67 Redundancy Multi-chassis Sync Peer Field Descriptions

Label	Description
DB Sync State	Displays the database state of the synchronization.
Num Entries	Displays the number of entries on local router.
Lcl Deleted Entries	Displays the number of deleted entries made at the local router.
Alarm Entries	Displays the alarm entries on the local router.
Rem Num Entries	Displays the number of entries on the remote router.
Rem Lcl Deleted Entries	Displays the number of locally deleting entries made by the remote router.
Rem Alarm Entries	Displays alarm entries on the remote router.

Sample Output

```

*A:subscr_mgt_2# show redundancy multi-chassis sync peer 10.10.10.20
=====
Multi-chassis Peer Table
=====
Peer
-----
Peer IP Address      : 10.10.10.20
Description          : Mc-Lag peer 10.10.10.20
Authentication       : Disabled
Source IP Address    : 0.0.0.0
Admin State          : Enabled
-----
Sync-status
-----
Client Applications  : SUBMGMT
Sync Admin State     : Up
Sync Oper State      : Up
DB Sync State        : inSync
Num Entries          : 1
Lcl Deleted Entries  : 0
Alarm Entries        : 0
Rem Num Entries      : 1
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
=====
MCS Application Stats
=====
Application          : igmp
Num Entries          : 0
Lcl Deleted Entries  : 0
Alarm Entries        : 0
-----
Rem Num Entries      : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
-----

```

```

Application          : igmpSnooping
Num Entries          : 0
Lcl Deleted Entries  : 0
Alarm Entries        : 0
-----
Rem Num Entries      : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
-----
Application          : subMgmt
Num Entries          : 1
Lcl Deleted Entries  : 0
Alarm Entries        : 0
-----
Rem Num Entries      : 1
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
-----
Application          : srrp
Num Entries          : 0
Lcl Deleted Entries  : 0
Alarm Entries        : 0
-----
Rem Num Entries      : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
=====
*A:subscr_mgt_2#

```

detail

- Syntax** **detail**
- Context** show>redundancy>multi-chassis>peer
- Description** This command displays detailed peer information.
- Output** The following table describes show redundancy multi-chassis sync detail output fields:

Table 68 Redundancy Multi-chassis Sync Peer Detail Field Descriptions

Label	Description
Peer IP Address	Displays the multi-chassis redundancy peer.
Description	The text string describing the peer.
Authentication	If configured, displays the authentication key used between this node and the multi-chassis peer.
Source IP Address	Displays the source address used to communicate with the multi-chassis peer.
Admin State	Displays the administrative state of the peer.

Table 68 Redundancy Multi-chassis Sync Peer Detail Field Descriptions

Label	Description (Continued)
Client Applications	Displays the list of client applications synchronized between routers.
Sync Admin State	Displays the administrative state of the synchronization.
Sync Oper State	Displays the operation state of the synchronization.
DB Sync State	Displays the database state of the synchronization.
Num Entries	Displays the number of entries on local router.
Lcl Deleted Entries	Displays the number of deleted entries made at the local router.
Alarm Entries	Displays the alarm entries on the local router.
Rem Num Entries	Displays the number of entries on the remote router.
Rem Lcl Deleted Entries	Displays the number of locally deleting entries made by the remote router.
Rem Alarm Entries	Displays alarm entries on the remote router.

Sample Output

```

*A:subscr_mgt_2# show redundancy multi-chassis sync peer 10.10.10.20 detail
=====
Multi-chassis Peer Table
=====
Peer
-----
Peer IP Address      : 10.10.10.20
Description          : Mc-Lag peer 10.10.10.20
Authentication       : Disabled
Source IP Address    : 0.0.0.0
Admin State          : Enabled
-----
Sync-status
-----
Client Applications  : SUBMGMT
Sync Admin State     : Up
Sync Oper State      : Up
DB Sync State        : inSync
Num Entries          : 1
Lcl Deleted Entries  : 0
Alarm Entries        : 0
Rem Num Entries      : 1
Rem Lcl Deleted Entries : 0
Rem Alarm Entries    : 0
=====
MCS Application Stats
=====
Application          : igmp
Num Entries          : 0

```

```

Lcl Deleted Entries      : 0
Alarm Entries           : 0
-----
Rem Num Entries         : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries       : 0
-----
Application             : igmpSnooping
Num Entries             : 0
Lcl Deleted Entries     : 0
Alarm Entries           : 0
-----
Rem Num Entries         : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries       : 0
-----
Application             : subMgmt
Num Entries             : 1
Lcl Deleted Entries     : 0
Alarm Entries           : 0
-----
Rem Num Entries         : 1
Rem Lcl Deleted Entries : 0
Rem Alarm Entries       : 0
-----
Application             : srrp
Num Entries             : 0
Lcl Deleted Entries     : 0
Alarm Entries           : 0
-----
Rem Num Entries         : 0
Rem Lcl Deleted Entries : 0
Rem Alarm Entries       : 0
=====
Ports synced on peer 10.10.10.20
=====
Port/Encap              Tag
-----
lag-1                   test123
=====
*A:subscr_mgt_2#

```

synchronization

Syntax **synchronization**

Context show>redundancy

Description This command displays redundancy synchronization times.

Output

Sample Output

```
A:ALA-48>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:ALA-48>show>redundancy#

```

satellite

Syntax	satellite
Context	show>system
Description	This command displays a list of configured Ethernet satellites including information about the satellite's esat-ID, satellite type, and state.
Output	

Sample Output

```

A:Dut-A# show system satellite

=====
Satellite Information
=====
SatID      Provisioned Type          Admin      Oper
           Equipped Type (if different)  State      State
-----
esat-1     es48-lgb-sfp                    up         provisioned
           (not equipped)
esat-20    es48-lgb-sfp                    up         up
-----
No. of Satellites: 2
=====

```

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.
owner script-owner — Displays information for the specified script owner.
- Output** The following table describes the show script output fields.

Table 69 Show script output

Label	Description
Script	Displays the name of the script.
Script owner	Displays the owner name of script.
Administrative status	Enabled — Administrative status is enabled.
	Disabled — Administratively disabled.
Operational status	Enabled — Operational status is enabled.
	Disabled — Operationally disabled.
Script source location	Displays the location of scheduled script.
Last script error	Displays the system time of the last error.
Last change	Displays the system time of the last change.

Sample Output

```
A:sim1>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://*****:*****@100.100.100.1/home/testlab_bgp
                       /test1.cfg
Last script error     : none
Last change           : 2015/01/07 17:10:03
=====
A:sim1>show>cron#
```

script-policy

- Syntax** **script-policy** *script-policy-name* [**owner** *owner-name*]
script-policy run-history [*run-state*]
- Context** show>system>script-control
- Description** This command displays script policy information.
- Parameters** *script-policy-name* — Displays policy information for the specified script.
owner *owner-name* — Displays information for the specified script owner.
Default TiMOS CLI
run-state — Displays information for script policies in the specified state.
Values executing | initializing | terminated
- Output** The following table describes script policy output fields.

Table 70 Script Policy Output

Label	Description
Script policy	Displays the name of the script policy.
Script policy owner	The name of the script policy owner.
Administrative status	Enabled — Administrative status is enabled. Disabled — Administrative status is disabled.
Script	The name of the script.
Script owner	The name of the script owner.
Script source location	Displays the location of scheduled script.
Max running allowed	Displays the maximum number of allowed sessions.
Max completed run histories	Displays the maximum number of sessions previously run.
Max lifetime allowed	Displays the maximum amount of time the script may run.
Completed run histories	Displays the number of completed sessions.
Executing run histories	Displays the number of sessions in the process of executing.
Initializing run histories	Displays the number of sessions ready to run/queued but not executed.

Table 70 Script Policy Output (Continued)

Label	Description (Continued)
Max time tun history saved	Displays the maximum amount of time to keep the results from a script run.
Last change	Displays the system time a change was made to the configuration.

Sample Output

```
*A:Redundancy# show system script-control script-policy run-history terminated
=====
Script-policy Run History
=====
Script policy "test"
Owner "TiMOS CLI"
-----

Script Run #17
-----
Start time : 2006/11/06 20:30:09 End time : 2006/11/06 20:35:24
Elapsed time : 0d 00:05:15 Lifetime : 0d 00:00:00
State : terminated Run exit code : noError
Result time : 2006/11/06 20:35:24 Keep history : 0d 00:49:57
Error time : never
Results file : ftp://*:~@192.168.15.18/home/testlab_bgp/cron/_20061106-203008.
out
Run exit : Success
-----

Script Run #18
-----
Start time : 2006/11/06 20:35:24 End time : 2006/11/06 20:40:40
Elapsed time : 0d 00:05:16 Lifetime : 0d 00:00:00
State : terminated Run exit code : noError
Result time : 2006/11/06 20:40:40 Keep history : 0d 00:55:13
Error time : never
Results file : ftp://*:~@192.168.15.18/home/testlab_bgp/cron/_20061106-203523.
out
Run exit : Success
-----

*A:Redundancy#

*A:Redundancy# show system script-control script-policy run-history executing
=====
Script-policy Run History
=====
Script policy "test"
Owner "TiMOS CLI"
-----

Script Run #20
-----
Start time : 2006/11/06 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/_20061106-204559.
```

```
out
=====
*A:Redundancy#

*A:Redundancy# 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:Redundancy#
```

uptime

Syntax	uptime
Context	show
Description	This command displays the time since the system started.
Output	The following table describes uptime output fields.

Table 71 Uptime Output

Label	Description
System Up Time	Displays the length of time the system has been up in days, hr:min:sec format.

Sample Output

```
A:ALA-1# show uptime
System Up Time      : 11 days, 18:32:02.22 (hr:min:sec)

A:ALA-1#
```

switch-fabric

- Syntax** **switch-fabric** [**exclude-sfm** *sfm-list*]
switch-fabric high-bandwidth-multicast
- Context** show>system
- Description** This command displays switch fabric information.
- Parameters** *sfm-list* — Specifies which SFMs to exclude from the displayed information.
Values “A”, “B”, “A,B”, “1”, “2”, and “1,2”
high-bandwidth-multicast — Displays MDA information about the switch-fabric plane’s high bandwidth multicast traffic tap allocation.
- Output** The following table describes switch-fabric output fields for 12-slot and 7-slot chassis models.

Table 72 Switch fabric output

Label	Description
Slot/MDA	Displays the fabric slot within a chassis in the system. The CPM cards and XCM/IOM cards cannot be physically inserted into the switch fabric card slots.
Min. Forwarding Capacity	Displays the minimum forwarding capacity of the slot and XMA/MDA as a percentage.
Max. Forwarding Capacity	Displays the maximum forwarding capacity of the slot and XMA/MDA as a percentage.

Sample Output

The following is an example for the 7750 SR:

```
A:ALA-7# show system switch-fabric
=====
Switch Fabric
=====
Slot/Mda Min. Forwarding Capacity Max. Forwarding Capacity
-----
1/1 100% 100%
1/2 100% 100%
2/1 100% 100%
2/2 100% 100%
3/1 100% 100%
3/2 100% 100%
4/1 100% 100%
4/2 100% 100%
5/1 100% 100%
5/2 100% 100%
A 100% 100%
B 100% 100%
=====
A:ALA-7#

A:ALA-12# show system switch-fabric
```

sync-if-timing

- Syntax** sync-if-timing
- Context** show>system
- Description** This command displays synchronous interface timing operational information.
- Output** The following table describes sync-if-timing output fields.

Table 73 System Timing Output

Label	Description
System Status CPM A/B	Indicates the present status of the synchronous timing equipment subsystem (SETS). Not Present — Only shown on systems without central clocks (7450 ESS-1) Master Freerun — The clock is in free-run because it hasn't had a qualified input reference to lock to Master Holdover — The clock was locked to an input reference but has lost all qualified input references and is in holdover. Master Locked — The clock is locked to an input reference Acquiring — The clock is training to a qualified input reference.

Table 73 **System Timing Output (Continued)**

Label	Description (Continued)
Reference Input Mode	<p>Revertive — Indicates that for a re-validated or a newly validated reference source which has a higher priority than the currently selected reference has reverted to the new reference source.</p> <p>Non-revertive — The clock cannot revert to a higher priority clock if the current clock goes offline.</p>
Quality Level Selection	<p>Indicates whether the ql-selection command has been enabled or disabled. If this command is enabled, then the reference is selected first using the QL value, then by the priority reference order. If this command is not enabled, then the reference is selected by the priority reference order.</p>
Reference Selected	<p>Indicates which reference has been selected:</p> <ul style="list-style-type: none"> • ref1, ref2 - (for all chassis) • BITS A, BITS B: <ul style="list-style-type: none"> – 7450 ESS-7/12 – 7750 SR-7/12 – 7750 SR-12e – 7750 SR-1e/2e/3e – 7750 SR-a4/8 – 7950 XRS-16/20 – 7950 XRS-40 • BITS C, BITS D - (7950 XRS-40)

Table 73 **System Timing Output (Continued)**

Label	Description (Continued)
	<ul style="list-style-type: none"> • Mate CPM (BITS A), Mate CPM (BITS B) - show>system>sync-if-timing>standby: <ul style="list-style-type: none"> – 7450 ESS-7/12 – 7750 SR-7/12 – 7750 SR-12e – 7750 SR-1e/2e/3e – 7750 SR-a4/8 – 7950 XRS-16/20 – 7950 XRS-40 • Mate CPM (BITS A), Mate CPM (BITS B) - show>system>sync-if-timing: <ul style="list-style-type: none"> – 7450 ESS-7/12 – 7750 SR-7/12 – 7750 SR-12e – 7750 SR-a4/8 • Mate CPM (none) - show>system>sync-if-timing>standby when standby locked to active which is freerun or holdover - (for all chassis) • Mate CPM (ref1), Mate CPM (ref2) - show>system>sync-if-timing>standby when standby locked to active which is locked to ref1 or ref2: <ul style="list-style-type: none"> – 7750 SR-7/12 – 7450 ESS-7/12 – 7750 SR-12e – 7750 SR-1e/2e/3e – 7750 SR-a4/8 – 7950 XRS-16/20/40 – BITS 1, BITS2 - (7750 SR-c4 only)
System Quality Level	Indicates the quality level being generated by the system clock.
Current Frequency Offset	(value) The frequency offset of the currently selected timing reference in parts per million.
Reference Order	ref1, ref2, bits — Indicates that the priority order of the timing references.

Table 73 System Timing Output (Continued)

Label	Description (Continued)
Reference Mate CPM	Data within this block represents the status of the timing reference provided by the Mate CPM. This will be the BITS input from the standby CPM.
Admin Status	down — The ref1 or ref2 configuration is administratively shutdown. up — The ref1 or ref2 configuration is administratively enabled. diag — Indicates the reference has been forced using the force-reference command.
Quality Level Override	Indicates whether the QL value used to determine the reference was configured directly by the user.
Rx Quality Level	Indicates the QL value received on the interface. <ul style="list-style-type: none"> • inv - SSM received on the interface indicates an invalid code for the interface type. • unknown - No QL value was received on the interface.
Qualified for Use	Indicates whether the reference has been qualified to be used as a source of timing for the node.
Not Qualified Due To	Indicates the reason why the reference has not been qualified: <ul style="list-style-type: none"> • disabled • LOS • OOPIR • OOF
Selected for Use	Indicates whether the method is presently selected.
Not Selected Due To	Indicates the reason why the method is not selected: <ul style="list-style-type: none"> • disabled • not qualified • previous failure • LOF • AIS-L • validating • on standby • ssm quality
Source Port	Identifies the Source port for the reference.
Interface Type	The interface type configured for the BITS port.
Framing	The framing configured for the BITS port.

Table 73 **System Timing Output (Continued)**

Label	Description (Continued)
Line Coding	The line coding configured for the BITS port.
Line Length	The line length value of the BITS output.
Output Admin Status	down — The BITS output is administratively shutdown. up — The BITS output is administratively enabled.
Output Source	The source to be used to provide the signal on the BITS output port. line reference — unfiltered recovered line reference. internal clock — filtered node clock output.
Output Reference Selected	The reference selected as the source for the BITS output signal (ref1, ref2, or PTP).
TX Quality Level	QL value for BITS output signal.

Sample Output

The following system example shows:

- **sync-if timing**, or
- **sync-if-timing "A"** when the SETS reference on the active CPM-A locks to BITS A, or
- **sync-if-timing "B"** when the SETS reference on the active CPM-B locks to BITS A



Note: The following output applies only to the 7750 SR-1e/2e/3e and 7950 XRS-16/20/40 platforms.

```
*A:Dut-B# show system sync-if-timing or show system sync-if-timing "A"
=====
System Interface Timing Operational Info
=====
System Status CPM A                : Master Locked
  Reference Input Mode              : Revertive
  Quality Level Selection           : Disabled
  Reference Selected                : BITS A
  System Quality Level              : prc
  Current Frequency Offset (ppm)   : +0

Reference Order                    : bits ref1 ref2

Reference Input 1
  Admin Status                     : up
  Rx Quality Level                  : prc
  Quality Level Override            : none
  Qualified For Use                 : Yes
```

```

Selected For Use           : No
  Not Selected Due To      :      on standby
Source Port                : 1/1/5

Reference Input 2
  Admin Status             : up
  Rx Quality Level         : prc
  Quality Level Override   : none
  Qualified For Use        : Yes
  Selected For Use         : No
    Not Selected Due To    :      on standby
Source Port                : 3/1/5

Reference BITS A
  Input Admin Status       : up
  Rx Quality Level         : prc
  Quality Level Override   : none
  Qualified For Use        : Yes
  Selected For Use         : Yes
  Interface Type           : E1
  Framing                  : PCM31 CRC
  Line Coding              : HDB3
  SSM Bit                  : 8
  Output Admin Status      : up
  Output Source            : line reference
  Output Reference Selected : refl
  Tx Quality Level         : prc

Reference BITS B
  Input Admin Status       : up
  Rx Quality Level         : prc
  Quality Level Override   : none
  Qualified For Use        : Yes
  Selected For Use         : No
    Not Selected Due To    :      on standby
  Interface Type           : E1
  Framing                  : PCM31 CRC
  Line Coding              : HDB3
  SSM Bit                  : 8
  Output Admin Status      : up
  Output Source            : line reference
  Output Reference Selected : refl
  Tx Quality Level         : prc
=====

```

The following system example shows:

- **sync-if timing** standby, or
- **sync-if-timing** “B” when the SETS reference on the standby CPM-B locks to Mate CPM (BITS A), or
- **sync-if-timing** “A” when the SETS reference on the standby CPM-A locks to Mate CPM (BITS A)



Note: The following output applies only to the 7750 SR-1e/2e/3e and 7950 XRS-16/20/40 platforms.

```

-----
*A:Dut-B# show system sync-if-timing standby or show system sync-if-timing "B"
=====
System Interface Timing Operational Info
=====
System Status CPM B                : Master Locked
  Reference Input Mode              : Revertive
  Quality Level Selection           : Disabled
  Reference Selected                : Mate CPM (BITS A)
  System Quality Level              : prc
  Current Frequency Offset (ppm)   : +0sync-if-timing "A

Reference Order                    : bits ref1 ref2

Reference Mate CPM
  Qualified For Use                 : Yes
  Selected For Use                  : Yes

Reference Input 1
  Admin Status                     : up
  Rx Quality Level                  : prc
  Quality Level Override            : none
  Qualified For Use                 : Yes
  Selected For Use                  : No
  Not Selected Due To              :      on standby
  Source Port                      : 1/1/5

Reference Input 2
  Admin Status                     : up
  Rx Quality Level                  : prc
  Quality Level Override            : none
  Qualified For Use                 : Yes
  Selected For Use                  : No
  Not Selected Due To              :      on standby
  Source Port                      : 3/1/5

Reference BITS A
  Input Admin Status               : up
  Rx Quality Level                  : prc
  Quality Level Override            : none
  Qualified For Use                 : Yes
  Selected For Use                  : No
  Not Selected Due To              :      on standby
  Interface Type                   : E1
  Framing                          : PCM31 CRC
  Line Coding                       : HDB3
  SSM Bit                          : 8
  Output Admin Status              : up
  Output Source                    : line reference
  Output Reference Selected        : ref1
  Tx Quality Level                 : prc

```

```
Reference BITS B
  Input Admin Status      : up
  Rx Quality Level        : prc
  Quality Level Override  : none
  Qualified For Use       : Yes
  Selected For Use        : No
    Not Selected Due To   :      on standby
  Interface Type          : E1
  Framing                 : PCM31 CRC
  Line Coding             : HDB3
  SSM Bit                 : 8
  Output Admin Status     : up
  Output Source           : line reference
  Output Reference Selected : ref1
  Tx Quality Level        : prc
=====
```

The following system example shows:

- **sync-if timing**, or
- **sync-if-timing "A"** when the SETS reference on the active CPM-A locks to BITS B, or
- **sync-if-timing "B"** when the SETS reference on the active CPM-B locks to BITS B



Note: The following output applies only to the 7750 SR-1e/2e/3e and 7950 XRS-16/20/40 platforms.

```
-----
*A:Dut-B# show system sync-if-timing or show system sync-if-timing "A"
=====
System Interface Timing Operational Info
=====
System Status CPM A      : Master Locked
  Reference Input Mode    : Non-revertive
  Quality Level Selection : Disabled
  Reference Selected      : BITS B
  System Quality Level    : prc
  Current Frequency Offset (ppm) : +0

Reference Order          : bits ref1 ref2

Reference Input 1
  Admin Status          : up
  Rx Quality Level      : prc
  Quality Level Override : none
  Qualified For Use      : Yes
  Selected For Use      : No
    Not Selected Due To :      on standby
  Source Port           : 1/1/5

Reference Input 2
  Admin Status          : up
  Rx Quality Level      : prc
```

```

Quality Level Override      : none
Qualified For Use          : Yes
Selected For Use           : No
    Not Selected Due To    :      on standby
Source Port                : 3/1/5

Reference BITS A
Input Admin Status         : up
Rx Quality Level           : prc
Quality Level Override     : none
Qualified For Use          : Yes
Selected For Use           : No
    Not Selected Due To    :      previous failure
Interface Type             : E1
Framing                    : PCM31 CRC
Line Coding                : HDB3
SSM Bit                    : 8
Output Admin Status        : up
Output Source              : line reference
Output Reference Selected  : refl
Tx Quality Level           : prc

Reference BITS B
Input Admin Status         : up
Rx Quality Level           : prc
Quality Level Override     : none
Qualified For Use          : Yes
Selected For Use           : Yes
Interface Type             : E1
Framing                    : PCM31 CRC
Line Coding                : HDB3
SSM Bit                    : 8
Output Admin Status        : up
Output Source              : line reference
Output Reference Selected  : refl
Tx Quality Level           : prc
=====

```

The following system example shows:

- **sync-if timing** standby, or
- **sync-if-timing "B"** when the SETS reference on the standby CPM-B locks to Mate CPM (BITS B), or
- **sync-if-timing "A"** when the SETS reference on the standby CPM-A locks to Mate CPM (BITS B)



Note: The following output applies only to the 7750 SR-1e/2e/3e and 7950 XRS-16/20/40 platforms.

```

-----
*A:Dut-B# show system sync-if-timing standby or show system sync-if-timing "B"
=====

```

```

System Interface Timing Operational Info
=====
System Status CPM B                : Master Locked
  Reference Input Mode              : Non-revertive
  Quality Level Selection           : Disabled
  Reference Selected                 : Mate CPM (BITS B)
  System Quality Level              : prc
  Current Frequency Offset (ppm)    : +0

Reference Order                     : bits ref1 ref2

Reference Mate CPM
  Qualified For Use                 : Yes
  Selected For Use                 : Yes

Reference Input 1
  Admin Status                     : up
  Rx Quality Level                 : prc
  Quality Level Override           : none
  Qualified For Use                 : Yes
  Selected For Use                 : No
    Not Selected Due To           :      on standby
  Source Port                      : 1/1/5

Reference Input 2
  Admin Status                     : up
  Rx Quality Level                 : prc
  Quality Level Override           : none
  Qualified For Use                 : Yes
  Selected For Use                 : No
    Not Selected Due To           :      on standby
  Source Port                      : 3/1/5

Reference BITS A
  Input Admin Status               : up
  Rx Quality Level                 : prc
  Quality Level Override           : none
  Qualified For Use                 : Yes
  Selected For Use                 : No
    Not Selected Due To           :      previous failure
  Interface Type                   : E1
  Framing                         : PCM31 CRC
  Line Coding                      : HDB3
  SSM Bit                         : 8
  Output Admin Status              : up
  Output Source                    : line reference
  Output Reference Selected        : ref1
  Tx Quality Level                 : prc

Reference BITS B
  Input Admin Status               : up
  Rx Quality Level                 : prc
  Quality Level Override           : none
  Qualified For Use                 : Yes
  Selected For Use                 : No
    Not Selected Due To           :      on standby
  Interface Type                   : E1
  Framing                         : PCM31 CRC
  Line Coding                      : HDB3

```

```

SSM Bit                : 8
Output Admin Status    : up
Output Source          : line reference
Output Reference Selected : refl
Tx Quality Level       : prc

```

=====

synchronization

Syntax **synchronization**

Context show>redundancy>synchronization

Description This command displays redundancy synchronization times.

Output The following table describes redundancy synchronization output fields.

Table 74 Synchronization Output

Label	Description
Standby Status	Displays the status of the standby CPM.
Last Standby Failure	Displays the timestamp of the last standby failure.
Standby Up Time	Displays the length of time the standby CPM has been up.
Failover Time	Displays the timestamp when the last redundancy failover occurred causing a switchover from active to standby CPM. If there is no redundant CPM 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 CPMs 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 CPMs.
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.

Sample Output

```
A:ALA-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:ALA-1>show>redundancy#
```

5.23.2.2 Debug Commands

sync-if-timing

Syntax	sync-if-timing
Context	debug
Description	The context to debug synchronous interface timing references.

force-reference

Syntax	force-reference {ref1 ref2 bits bits1 bits2 bitsa bitsb ptp} no force-reference
Context	debug>sync-if-timing
Description	<p>This command allows an operator to force the system synchronous timing output to use a specific reference.</p> <p>The debug sync-if-timing force-reference command should only be used to test and debug problems. Network synchronization problems may appear if network elements are left with this manual override setting. Once the system timing reference input has been forced, it may be cleared using the no force-reference command.</p> <p>The CPM clock can be forced to use a specific input reference using the force-reference command.</p>

When the command is executed, the CPM clock on the active CPM immediately switches its input reference to that specified by the command. If the specified input is not available (shutdown), or in a disqualified state, the CPM clock shall use the next qualified input reference based on the selection rules.

This command also affects the BITS output port on the active CPM. If the BITS output port selection is set to line-reference and the reference being forced is not the BITS input port, then the system uses the forced reference to generate the signal out the BITS output port. If the BITS output port selection is set to internal-clock, then the system uses the output of the CPM clock to generate the signal for the BITS output port.

On a CPM activity switch, the force command is cleared and normal reference selection is determined.

Debug configurations are not saved between reboots.

The 7750 SR-c4 has two BITS input ports on the CFM. The force reference command on this system allows the selection of the specific port.

7750 SR-c4 CLI Syntax: **debug>sync-if-timing>force-reference {ref1 | ref2 | bits | bits1 | bits a | bits b}**

- Parameters**
- ref1** — The clock will use the first timing reference.
 - ref2** — The clock will use the second timing reference.
 - bits** — The clock will use the external network interface on the active CPM to be the highest priority input.
 - bits1** — (7750 SR-c4) The clock will use the bits1 timing reference.
 - bits2** — (7750 SR-c4) The clock will use the bits2 timing reference.
 - bitsa** — The clock will use the bitsa timing reference.
 - bitsb** — The clock will use the bitsb timing reference.
 - ptp** — The clock will use the PTP slave as the timing reference (applies to the 7450 ESS and 7750 SR).

system

- Syntax** [no] **system**
- Context** debug
- Description** This command displays system debug information.

http-connections

- Syntax** **http-connections** [*host-ip-address/mask*]

http-connections

Context	debug>system
Description	This command displays HTTP connections debug information.
Parameters	<i>host-ip-address/mask</i> — Displays information for the specified host IP address and mask.

ntp

Syntax	[no] router <i>router-instance</i> interface <i>ip-int-name</i>		
Context	debug>system		
Description	This command enables and configures debugging for NTP. The no form of the command disables debugging for NTP.		
Parameters	<i>router-instance</i> — specifies the router name or CPM router instance		
	<i>router-instance</i> : <i>router-name</i>		
	<i>router-name</i>	Base management <i>cpm-vr-name</i>	
	<i>cpm-vr-name</i>	[32 characters maximum]	
Default	Base		
	<i>ip-int-name</i> — Maximum 32 characters; must begin with a letter. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.		

persistence

Syntax	[no] persistence
Context	debug>system
Description	This command displays persistence debug information.

5.23.2.3 Tools Commands

redundancy

Syntax	redundancy
Context	tools>dump
Description	This command enables the context to dump redundancy parameters.

multi-chassis

Syntax	multi-chassis
Context	tools>dump>redundancy
Description	This command enables the context to dump multi-chassis parameters.

mc-endpoint

Syntax	mc-endpoint peer <i>ip-address</i>
Context	tools>dump>redundancy>multi-chassis
Description	This command dumps multi-chassis endpoint information.
Parameters	peer <i>ip-address</i> — Specifies the peer's IP address.
Output	

Sample Output

```
*A:Dut-B# tools dump redundancy multi-chassis mc-endpoint peer 3.1.1.3
MC Endpoint Peer Info
  peer addr           : 3.1.1.3
  peer name           : Dut-C
  peer name refs      : 1
  src addr conf       : Yes
  source addr         : 2.1.1.2
  num of mcep         : 1
  num of non-mcep     : 0
  own sess num        : 58ba0d39
  mc admin state      : Up
  tlv own mc admin state : Up
  tlv peer mc admin state : Up
  reachable           : Yes

  own sys priority    : 50
  own sys id          : 00:03:fa:72:c3:c0
```

```

peer sys priority          : 21
peer sys id                : 00:03:fa:c6:31:f8
master                     : No

conf boot timer            : 300
boot timer active          : No
conf ka intv               : 10
conf hold on num of fail   : 3
tlv own ka intv            : 10
tlv peer ka intv           : 10
ka timeout tmr active      : Yes
ka timeout tmr intvl       : 20
ka timeout tmr time left   : 4
peer ka intv               : 10
mc peer timed out          : No

initial peer conf rx       : Yes
peer-mc disabled           : No
initial peer conf sync     : Yes
peer conf sync             : Yes

own passive mode           : Disable
peer passive mode          : No

retransmit pending         : No
non-mcep retransmit pending : No
retransmit intvl           : 5
last tx time               : 1437130
last rx time               : 1437156

own bfd                    : Enable
peer bfd                   : Enable
bfd vrtr if                : 2
bfd handle                  : 1
bfd state                   : 3
bfd code                    : 0

```

*A:Dut-B#

mc-ring

Syntax	mc-ring mc-ring peer <i>ip-address</i> [ring <i>sync-tag</i>]
Context	tools>dump>redundancy>multi-chassis
Description	This command dumps multi-chassis ring information.
Parameters	peer <i>ip-address</i> — Specifies the peer IP address. ring <i>sync-tag</i> — Specifies the ring's sync-tag created in the config>redundancy>mc>peer>mcr> ring context.

sync-database

Syntax **sync-database** [**peer** *ip-address*] [**port** *port-id* | *lag-id*] [**sync-tag** *sync-tag*] [**application** *application*] [**detail**] [**type** *type*]

Context tools>dump>redundancy>multi-chassis

Description This command dumps MCS database information.

Parameters **peer** *ip-address* — Specifies the peer’s IP address.
port *port-id* | *lag-id* — Indicates the port or LAG ID to be synchronized with the multi-chassis peer.

Values

<i>port-id</i>	<i>slot/mda/port</i>		
	<i>eth-sat-id</i>	esat-id/slot/port	
		esat	keyword
		<i>id</i>	1 to 20
	<i>pxc-id</i>	pxc-id.sub-port	
		pxc	keyword
		<i>id</i>	1 to 64
		<i>sub-port</i>	a, b
<i>lag-id</i>	<i>lag-lag-id</i>		

sync-tag *sync-tag* — Specifies a synchronization tag to be used while synchronizing this port with the multi-chassis peer.

application *application* — Specifies a particular multi-chassis peer synchronization protocol application.

Values

dhcp-server:	local dhcp server
igmp:	Internet group management protocol
igmp-snooping:	igmp-snooping
mc-ring	multi-chassis ring
mld-snooping:	multicast listener discovery-snooping
srrp:	simple router redundancy protocol
sub-host-trk:	subscriber host tracking
sub-mgmt:	subscriber management

type *type* — Indicates the locally deleted or alarmed deleted entries in the MCS database per multi-chassis peer.

Values alarm-deleted, local-deleted

detail — Displays detailed information.

srrp-sync-database

Syntax	srrp-sync-database [instance <i>instance-id</i>] [peer <i>ip-address</i>]
Context	tools>dump>redundancy>multi-chassis
Description	This command dumps SRRP database information and applies to the 7450 ESS.
Parameters	peer <i>ip-address</i> — Specifies the peer's IP address. instance <i>instance-id</i> — Dumps information for the specified Subscriber Router Redundancy Protocol instance configured on this system. Values 1 to 4294967295

resource-usage

Syntax	resource-usage
Context	tools>dump
Description	This command enables the context to display system resource information, such as policers, including data for total, available, and free numbers for each resource.

card

Syntax	card [<i>slot-num</i>] card [<i>slot-num</i>] all
Context	tools>dump>resource-usage
Description	This command displays resource information for cards.
Parameters	<i>slot-num</i> — Specifies a card slot. all — Keyword to display all available information for the card, including resource usage information for all child objects of the card such as FPs and MDAs.

fp

Syntax	fp [<i>fp-number</i>]
Context	tools>dump>resource-usage>card
Description	This command displays resource information for FPs.

Parameters *fp-number* — Specifies an FP.

mda

Syntax **mda** [*mda-slot*]

Context tools>dump>resource-usage>card

Description This command displays resource information for MDAs.

Parameters *mda-slot* — Specifies an MDA slot.

system

Syntax **system** [**all**]

Context tools>dump>resource-usage

Description This command displays resource information for resources that are managed at the system level.

Parameters **all** — Keyword to display all system resource usage information, as well as resource usage information for all cards, FPs, and MDAs in the system.

system-resources

Syntax **system-resources** *slot-number*

Context tools>dump

Description The system-resources command has been deprecated and replaced by the **tools>dump>resource-usage** command. The **system-resources** command continues to be supported in the current release, but it is recommended to use the **resource-usage** command instead.

 This command displays system resource information.

Default N/A

Parameters *slot-number* — Specifies a specific slot to view system resources information.

set-role

Syntax **set-role** {**standalone** | **master** | **extension**}

Context tools>perform>chassis

Description	<p>This command sets the role of the 7950 XRS chassis from which the command is invoked.</p> <ul style="list-style-type: none">• When run on a standalone chassis this will update the EEPROM on the (one) Chassis backplane.• Master and Extension chassis are blocked if any SFMs are configured as type sfm-x20 (must be sfm-x20-b). The following message displays:• When the extension option is specified, the chassis will immediately reboot as part of the command. The following warning and prompt will be provided: <p>WARNING: You are about to provision the chassis as an XRS-40 Extension chassis. This chassis will immediately reboot after the command is executed. No CLI shell is available directly on an Extension chassis. An Extension chassis will not completely boot up unless it is properly cabled to and controlled by an XRS-40 Master chassis. Do you wish to proceed (yes/no) ?</p> <ul style="list-style-type: none">• When the master option is specified, the chassis will immediately reboot as part of the command. The Operational mode is not changed until a reboot is performed. The following warning and prompt will be provided: <p>WARNING: You are about to provision the chassis as an XRS-40 Master chassis. This chassis will immediately reboot after the command is execute</p> <p>Do you wish to proceed (yes/no) ?</p> <ul style="list-style-type: none">• When the master or extension options are specified and the chassis has any SFM slots with a configured type of sfm-x20, then the command will fail with the following message: <p>Configured sfm-type of sfm-x20 is not compatible with XRS-40 mode operation.</p> <p>If you want to change the role of the chassis anyways, you can deconfigure the SFMs and then change the role.</p>
--------------------	---

mgmt-ethernet

Syntax	mgmt-ethernet
Context	tools>perform>redundancy>mgmt-ethernet
Description	This command triggers redundancy mode, just as if the management Ethernet port of the primary CPM has gone down. The router will revert if the management Ethernet port of the primary CPM has been up for the revert duration.

mixed-mode-upgrade

Syntax	mixed-mode-upgrade [<i>slot-list</i>] [now]
Context	tools>perform>system

Description	<p>This command initiates the upgrade process to enable mixed-mode in a 7450 ESS-7 or ESS-12.</p> <p>Executing this command will (as one action), enable the system state of mixed-mode and enable SR capabilities on the IOMs or IMMs located in the slots specified in the slot list. This will result in rebooting of the IOMs and IMMs located in the specified slots.</p> <p>If any of the IOMs or IMMs located in the specified slot-list are not IOM3-XP or later, this command will fail.</p> <p>This command can only be used to enable the mixed-mode state. It can not be used to reverse the state.</p>
Default	capability ess on a 7450 ESS chassis and capability sr on a 7750 SR chassis
Parameters	<p><i>slot-list</i> — List of slots to be upgraded to 7750 IOM3/IMM functionality. This parameter is required to modify the mode in which the IOM3/IMMs function and will require a reboot of the IOM3/IMMs in the designated slot.</p> <p>now — This optional keyword can be added to the interactive command to force the command to be executed immediately without further question. If this keyword is not present, then the user will be presented with a question to ensure they understand that as a result of this command, the associated slots will be reset immediately to enable mixed mode.</p>

set-fabric-speed

Syntax	set-fabric-speed <i>speed</i>
Context	tools>perform>system
Description	This command sets fabric speed for the 7750 SR. With the introduction of SFM5-12e and the mini-SFM5-12e, a new tools command (set-fabric-speed) was added to set the fabric operating speed. (tools command does not apply to SFM4-12e) fabric-speed-a).
Parameters	<p><i>fabric-speed-a</i> — The 7750 SR-12e chassis defaults to the fabric-speed-a when initially deployed with SFM5-12e. It operates at 200GB per slot which permits a mixture of FP2/FP3 based cards to co-exist.</p> <p><i>fabric-speed-b</i> — Enables the 7750 SR-12e to operate at up to 400 Gb/s, for which all cards in the 7750 SR-12e are required to be T3 based (FP3 IMM and/or IOM3-XP-C). The system will not support any FP2 based cards when the chassis is set to fabric-speed-b.</p>

sfm-interco-test

Syntax	sfm-interco-test [<i>sfm x</i>]
Context	tools>perform>system>inter-chassis>

Description Use this command to run inter-chassis SFM loopback tests for the 7950 XRS.

Run on an out-of-service standalone chassis that will later become the Extension chassis of an XRS-40 system. The out of service chassis (Chassis 1 – future Master chassis) must be connected by means of SFM interconnect links (cable bundles) before this test is run. This test operates without requiring any XCMs in either chassis, but they can be present.

The test should not be initiated from Chassis 1.

The following conditions must be satisfied for the test to be permitted:

- The system must be in standalone mode; error message:

`The test can only be performed on a standalone system`

- The system must have only XRS-40 compatible SFMs provisioned; error message:

`The chassis can not have SFMs with a configured type of sfm-x20s-b
when performing the test`

- All provisioned SFMs must be operational; error message:

`All provisioned SFMs must be operational before performing the test`

- The same test cannot be running in another session (i.e. only one test can be executed at a time); error message:

`The test is already in-progress in another session`

Other notes (which are also relayed to the operator when the test is attempted):

- All provisioned XCMs will be reset at the start of the test and will be held in the *booting* state until the test has completed.
- All SFMs will be cleared when the operator exits the test. This will trigger a reset of the XCMs and the standby CPM.

Output

Sample Output

```
*A:Dut-A# tools perform system inter-chassis sfm-interco-test
WARNING: This test is intended for an out-of-service standalone chassis that is
going to later become the extension chassis of an XRS-40 system.
```

```
At the start of the test, all provisioned IOMs will be reset and will be held
in the 'booting' state until the test has completed.
```

```
While the test is running avoid altering this system or the attached system
(e.g. do not shutdown, clear, or remove the CPMs/SFMs/IOMs and do not issue
CPM switchovers)
```

```
Once testing has completed all SFMs in this system will be cleared.
```

Do you wish to proceed (y/n)? y
 Clearing provisioned IOMs ...
 Test executing ...
 Displaying results

=====						
SFM Interconnect Port Summary						
=====						
SFM	SFM Oper State	IcPort Num	IcPort Oper State	Module Inserted	Degrade State	Miscon Info SFM IcPort

1	up	1	up	yes	none	
1	up	2	up	yes	none	
1	up	3	up	yes	none	
1	up	4	up	yes	none	
1	up	5	up	yes	none	
1	up	6	up	yes	none	
1	up	7	up	yes	none	
1	up	8	up	yes	none	
1	up	9	up	yes	none	
1	up	10	up	yes	none	
1	up	11	up	yes	none	
1	up	12	up	yes	none	
1	up	13	up	yes	none	
1	up	14	up	yes	none	
2	up	1	up	yes	none	
2	up	2	up	yes	none	
2	up	3	up	yes	none	
2	up	4	up	yes	none	
2	up	5	up	yes	none	
2	up	6	up	yes	none	
2	up	7	up	yes	none	
2	up	8	up	yes	none	
2	up	9	up	yes	none	
2	up	10	up	yes	none	
2	up	11	up	yes	none	
2	up	12	up	yes	none	
2	up	13	up	yes	none	
2	up	14	up	yes	none	
3	up	1	up	yes	none	
3	up	2	up	yes	none	
3	up	3	up	yes	none	
3	up	4	up	yes	none	
3	up	5	up	yes	none	
3	up	6	up	yes	none	
3	up	7	up	yes	none	
3	up	8	up	yes	none	
3	up	9	up	yes	none	
3	up	10	up	yes	none	
3	up	11	up	yes	none	
3	up	12	up	yes	none	
3	up	13	up	yes	none	
3	up	14	up	yes	none	
4	up	1	up	yes	none	
4	up	2	up	yes	none	
4	up	3	up	yes	none	
4	up	4	up	yes	none	
4	up	5	up	yes	none	

4	up	6	up	yes	none
4	up	7	up	yes	none
4	up	8	up	yes	none
4	up	9	up	yes	none
4	up	10	up	yes	none
4	up	11	up	yes	none
4	up	12	up	yes	none
4	up	13	up	yes	none
4	up	14	up	yes	none
5	up	1	up	yes	none
5	up	2	up	yes	none
5	up	3	up	yes	none
5	up	4	up	yes	none
5	up	5	up	yes	none
5	up	6	up	yes	none
5	up	7	up	yes	none
5	up	8	up	yes	none
5	up	9	up	yes	none
5	up	10	up	yes	none
5	up	11	up	yes	none
5	up	12	up	yes	none
5	up	13	up	yes	none
5	up	14	up	yes	none
6	up	1	up	yes	none
6	up	2	up	yes	none
6	up	3	up	yes	none
6	up	4	up	yes	none
6	up	5	up	yes	none
6	up	6	up	yes	none
6	up	7	up	yes	none
6	up	8	up	yes	none
6	up	9	up	yes	none
6	up	10	up	yes	none
6	up	11	up	yes	none
6	up	12	up	yes	none
6	up	13	up	yes	none
6	up	14	up	yes	none
7	up	1	up	yes	none
7	up	2	up	yes	none
7	up	3	up	yes	none
7	up	4	up	yes	none
7	up	5	up	yes	none
7	up	6	up	yes	none
7	up	7	up	yes	none
7	up	8	up	yes	none
7	up	9	up	yes	none
7	up	10	up	yes	none
7	up	11	up	yes	none
7	up	12	up	yes	none
7	up	13	up	yes	none
7	up	14	up	yes	none
8	up	1	up	yes	none
8	up	2	up	yes	none
8	up	3	up	yes	none
8	up	4	up	yes	none
8	up	5	up	yes	none
8	up	6	up	yes	none
8	up	7	up	yes	none
8	up	8	up	yes	none

```
8      up      9      up      yes      none
8      up     10      up      yes      none
8      up     11      up      yes      none
8      up     12      up      yes      none
8      up     13      up      yes      none
8      up     14      up      yes      none
=====

Correct any mis-cabling and replace any suspected faulty equipment. Press Q to
quit the test or any other key to run the test again. q
Test complete, clearing the SFMs to return them to normal operational state.
Done. Exiting test.
```

stop

- Syntax** **stop** [*script-policy-name*] [**owner** *script-policy-owner*] [**all**]
- Context** tools>perform>system>script-control>script-policy
- Description** This command stops the execution of scripts.
- Parameters** *script-policy-name* — Only stop scripts with the specified script-policy.
 owner *script-policy-owner* — Only stop scripts that are associated with script-policies with the specified owner.
 Default TiMOS CLI
 all — Keyword to stop all running scripts.

5.23.2.4 Clear Commands

application-assurance

- Syntax** **application-assurance**
- Context** clear
- Description** This command clears application assurance commands.

group

- Syntax** **group** *isa-aa-group-id* **statistics**
 group *isa-aa-group-id* **status**
- Context** clear>app-assure
- Description** This command clears application assurance group data.

Parameters *isa-aa-group-id* — Specifies the ISA-AA group index.

Values 1

status — Specifies that application assurance system statistics are cleared.

statistics — Specifies that application assurance statistics are cleared.

redundancy

Syntax **redundancy**

Context clear

Description This command enables the context to clear redundancy parameters.

multi-chassis

Syntax **multi-chassis**

Context clear>redundancy

Description This command enables the context to clear multi-chassis parameters.

mc-endpoint

Syntax **mc-endpoint endpoint** [*mcep-id*] **statistics**
mc-endpoint statistics
mc-endpoint peer [*ip-address*] **statistics**

Context clear>redundancy>multi-chassis

Description This command clears multi-chassis endpoint statistics.

Parameters **endpoint** *mcep-id* — Clears information for the specified multi-chassis endpoint ID.

Values 1 to 4294967295

peer *ip-address* — Clears information for the specified peer IP address.

statistics — Clears statistics for this multi-chassis endpoint.

mc-lag

Syntax **mc-lag** [**peer** *ip-address* [**lag** *lag-id*]]

Context clear>redundancy>multi-chassis

Description	This command clears multi-chassis Link Aggregation Group (LAG) information.
Parameters	peer <i>ip-address</i> — Clears the specified address of the multi-chassis peer. lag <i>lag-id</i> — Clears the specified LAG on this system. Values 1 to 100

mc-ring

Syntax	mc-ring
Context	clear>redundancy>multi-chassis
Description	This command clears multi-chassis ring data.

debounce

Syntax	debounce peer <i>ip-address</i> ring <i>sync-tag</i>
Context	clear>redundancy>multi-chassis
Description	This command clears multi-chassis ring operational state debounce history.
Parameters	<i>ip-address</i> — Clears debounce history for the specified IP address. ring <i>sync-tag</i> — Clears debounce history for the specified sync tag.

ring-nodes

Syntax	ring-nodes peer <i>ip-address</i> ring <i>sync-tag</i>
Context	clear>redundancy>multi-chassis>mcr
Description	This command clears multi-chassis ring unreferenced ring nodes.
Parameters	<i>ip-address</i> — Clears ring statistics for the specified IP address. ring <i>sync-tag</i> — Clears ring statistics for the specified sync tag.

statistics

Syntax	statistics
Context	clear>redundancy>multi-chassis>mcr
Description	This command clears multi-chassis ring

global

Syntax	global
Context	clear>redundancy>multi-chassis>mcr>statistics
Description	This command clears multi-chassis ring global statistics.

peer

Syntax	peer <i>ip-address</i>
Context	clear>redundancy>multi-chassis>mcr>statistics
Description	This command clears multi-chassis ring peer statistics.
Parameters	<i>ip-address</i> — Clears ring peer statistics for the specified IP address.

ring

Syntax	ring peer <i>ip-address</i> ring <i>sync-tag</i>
Context	clear>redundancy>multi-chassis>mcr>statistics
Description	This command clears multi-chassis ring statistics.
Parameters	<i>ip-address</i> — Clears ring statistics for the specified IP address. ring <i>sync-tag</i> — Clears ring statistics for the specified sync tag.

ring-node

Syntax	ring-node peer <i>ip-address</i> ring <i>sync-tag</i> node <i>ring-node-name</i>
Context	clear>redundancy>multi-chassis>mcr>statistics
Description	This command clears multi-chassis ring statistics.
Parameters	peer <i>ip-address</i> — Clears ring-node peer statistics for the specified IP address. ring <i>sync-tag</i> — Clears ring-node peer statistics for the specified sync-tag. node <i>ring-node-name</i> — Clears ring-node peer statistics for the specified ring node name.

ptp

Syntax	ptp inactive-peers ptp statistics ptp peer <i>ip_address</i> statistics
Context	clear>system
Description	This command clears PTP statistics.
Parameters	<i>inactive-peers</i> — Removes PTP peers which are not currently exchanging PTP packets with the router. peer <i>ip_address</i> statistics — Clears statistics for the specified peer. <i>statistics</i> — Clears all ptp statistics.

sync-database

Syntax	sync-database peer <i>ip-address</i> all application <i>application</i> sync-database peer <i>ip-address</i> {port <i>port-id</i> lag-id sync-tag <i>sync-tag</i>} application <i>application</i> sync-database peer <i>ip-address</i> {sdp <i>sdp-id</i> sync-tag <i>sync-tag</i>} application <i>application</i> sync-database peer <i>ip-address</i> sync-tag <i>sync-tag</i> application <i>application</i>
Context	clear>redundancy>multi-chassis
Description	This command clears multi-chassis sync database information.
Parameters	peer <i>ip-address</i> — Clears the specified address of the multi-chassis peer. port <i>port-id</i> — Clears the specified port ID of the multi-chassis peer. port <i>lag-id</i> — Clears the specified Link Aggregation Group (LAG) on this system. all — Clears all ports and/or sync tags. sync-tag <i>sync-tag</i> — Clears the synchronization tag used while synchronizing this port with the multi-chassis peer. application — Clears the specified application information that was synchronized with the multi-chassis peer. Values The following are values for the 7750 SR and 7950 XRS:

all:	All supported applications
dhcp-server:	local dhcp server
igmp:	internet group management protocol
igmp-snooping:	igmp-snooping
mc-ring:	multi-chassis ring
mld-snooping:	multicast listener discovery-snooping
srrp:	simple router redundancy protocol
sub-host-trk	subscriber host tracking
sub-mgmt:	subscriber management

Values

The following are values for the 7450 ESS:

all	All supported applications
igmp-snooping	igmp-snooping
mc-ring	multi-chassis ring
mld-snooping	multicast listener discovery-snooping
sub-host-trk	subscriber host tracking
sub-mgmt	subscriber management

screen

Syntax	screen
Context	clear
Description	This command allows an operator to clear the Telnet or console screen.

system

Syntax	system
Context	clear
Description	This command allows an operator to clear system information.

ptp

Syntax	ptp
Context	clear>system

Description	This command enables the context to clear Precision Timing Protocol (PTP) information.
--------------------	--

inactive-peers

Syntax	inactive-peers
Context	clear>system>ptp
Description	This command clears inactive peer information.

peer

Syntax	peer <i>ip-address</i> [router <i>router-instance</i>] statistics
Context	clear>system>ptp
Description	This command clears PTP peer information.
Parameters	<i>ip-address</i> — Clears information that specific to the address of the PTP 1588 peer. router <i>router-instance</i> — Clears information that is specific to a virtual router instance. statistics — Clears statistics information of the specified IP address.

port

Syntax	port <i>port-id</i> statistics
Context	clear>system>ptp
Description	This command clears PTP port information.
Parameters	port <i>port-id</i> — Clears the specified port ID. statistics — Clears statistics information of the specified port ID.

statistics

Syntax	statistics
Context	clear>system>ptp
Description	This command clears all PTP statistics.

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 [<i>script-policy-name</i>] [owner <i>owner-name</i>]
Context	clear>system>script-control>script-policy
Description	This command clears completed script run history entries.
Parameters	<i>script-policy-name</i> — Only clear history entries for the specified script-policy. owner <i>owner-name</i> — Only clear history entries for script-policies with the specified owner. Default TiMOS CLI

statistics

Syntax	statistics
Context	clear>system
Description	This command clears system specific statistics.

xmpp

Syntax	xmpp <i>xmpp-server-name</i>
Context	clear>system>statistics
Description	This command clears XMPP server statistics.

sync-if-timing

Syntax	sync-if-timing {ref1 ref2 bits}
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	ref1 — clears the first timing reference. ref2 — clears the second timing reference. bits — Clears the bits timing reference.

trace

Syntax	trace
Context	clear
Description	This command clears commands for traces.

6 Standards and Protocol Support



Note: The information presented is subject to change without notice.

Oracle assumes no responsibility for inaccuracies contained herein.

Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

Application Assurance (AA)

3GPP Release 12 (ADC rules over Gx interfaces)

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000, *Integrated Local Management Interface (ILMI) Version 4.0*

AF-PHY-0086.001, *Inverse Multiplexing for ATM (IMA) Specification Version 1.1*

AF-TM-0121.000, *Traffic Management Specification Version 4.1*

AF-TM-0150.00, *Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR*

GR-1113-CORE, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1*

GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3*

ITU-T I.432.1, *B-ISDN user-network interface - Physical layer specification: General characteristics (02/99)*

ITU-T I.610, *B-ISDN operation and maintenance principles and functions (11/95)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Border Gateway Protocol (BGP)

draft-hares-idr-update-attr-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-04, *Advertisement of Multiple Paths in BGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*
draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*
draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*
draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*
RFC 1772, *Application of the Border Gateway Protocol in the Internet*
RFC 1997, *BGP Communities Attribute*
RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
RFC 2439, *BGP Route Flap Damping*
RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
RFC 2858, *Multiprotocol Extensions for BGP-4*
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, *A Border Gateway Protocol 4 (BGP-4)*
RFC 4360, *BGP Extended Communities Attribute*
RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
RFC 4486, *Subcodes for BGP Cease Notification Message*
RFC 4659, *BGP/MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
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 (helper mode)*
RFC 4760, *Multiprotocol Extensions for BGP-4*
RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*
RFC 4893, *BGP Support for Four-octet AS Number Space*
RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*
RFC 5065, *Autonomous System Confederations for BGP*
RFC 5291, *Outbound Route Filtering Capability for BGP-4*
RFC 5575, *Dissemination of Flow Specification Rules*
RFC 5668, *4-Octet AS Specific BGP Extended Community*
RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*
RFC 6811, *Prefix Origin Validation*
RFC 7607, *Codification of AS 0 Processing*

Circuit Emulation

MEF-8, *Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks*, October 2004

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

Ethernet

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*

IEEE 802.1aq, *Shortest Path Bridging*

IEEE 802.1ax, *Link Aggregation*

IEEE 802.1D, *MAC Bridges*

IEEE 802.1p, *Traffic Class Expediting*

IEEE 802.1Q, *Virtual LANs*

IEEE 802.1s, *Multiple Spanning Trees*

IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*

IEEE 802.1X, *Port Based Network Access Control*

IEEE 802.3ab, *1000BASE-T*

IEEE 802.3ac, *VLAN Tag*

IEEE 802.3ad, *Link Aggregation*

IEEE 802.3ae, *10 Gb/s Ethernet*

IEEE 802.3ah, *Ethernet in the First Mile*

IEEE 802.3ba, *40 Gb/s and 100 Gb/s Ethernet*

IEEE 802.3i, *Ethernet*

IEEE 802.3u, *Fast Ethernet*

IEEE 802.3x, *Ethernet Flow Control*

IEEE 802.3z, *Gigabit Ethernet*

ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*

ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

Ethernet VPN (EVPN)

draft-ietf-bess-evpn-overlay-02, *A Network Virtualization Overlay Solution using EVPN*

draft-ietf-bess-evpn-prefix-advertisement-02, *IP Prefix Advertisement in EVPN*

draft-ietf-bess-evpn-proxy-arp-nd-00, *Operational Aspects of Proxy-ARP/ND in EVPN Networks*

draft-ietf-bess-evpn-vpls-seamless-integ-00, *(PBB-)EVPN Seamless Integration with (PBB-)VPLS*

draft-ietf-bess-evpn-vpws-06, *VPWS support in EVPN*

RFC 7432, *BGP MPLS-Based Ethernet VPN*

RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*

Frame Relay

ANSI T1.617 Annex D, *DSS1 - Signalling Specification For Frame Relay Bearer Service*

FRF.1.2, *PVC User-to-Network Interface (UNI) Implementation Agreement*

FRF.12, *Frame Relay Fragmentation Implementation Agreement*

FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*

FRF.5, *Frame Relay/ATM PVC Network Interworking Implementation*

FRF2.2, *PVC Network-to-Network Interface (NNI) Implementation Agreement*

ITU-T Q.933 Annex A, *Additional procedures for Permanent Virtual Connection (PVC) status management*

Generalized Multiprotocol Label Switching (GMPLS)

draft-ietf-ccamp-rsvp-te-srlg-collect-04, *RSVP-TE Extensions for Collecting SRLG Information*

RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 4204, *Link Management Protocol (LMP)*

RFC 4208, *Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*

RFC 4872, *RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*

Intermediate System to Intermediate System (IS-IS)

draft-ginsberg-isis-mi-bis-01, *IS-IS Multi-Instance* (single topology)
draft-ietf-isis-mi-02, *IS-IS Multi-Instance*
draft-ietf-isis-segment-routing-extensions-04, *IS-IS Extensions for Segment Routing*
draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*
ISO/IEC 10589:2002, Second Edition, Nov. 2002, *Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)*
RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
RFC 2973, *IS-IS Mesh Groups*
RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*
RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*
RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*
RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*
RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*
RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*
RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*
RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*
RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*
RFC 5304, *IS-IS Cryptographic Authentication*
RFC 5305, *IS-IS Extensions for Traffic Engineering TE*
RFC 5306, *Restart Signaling for IS-IS (helper mode)*
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 6213, *IS-IS BFD-Enabled TLV*
RFC 6232, *Purge Originator Identification TLV for IS-IS*
RFC 6233, *IS-IS Registry Extension for Purges*
RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*

Internet Protocol (IP) — Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*

RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*

RFC 7431, *Multicast-Only Fast Reroute*

RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

Internet Protocol (IP) — General

draft-grant-tacacs-02, *The TACACS+ Protocol*

draft-ietf-vrrp-unified-spec-02, *Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6*

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

RFC 951, *Bootstrap Protocol (BOOTP)*

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1350, *The TFTP Protocol (revision 2)*

RFC 1534, *Interoperation between DHCP and BOOTP*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

RFC 2349, *TFTP Timeout Interval and Transfer Size Options*

RFC 2428, *FTP Extensions for IPv6 and NATs*

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 3046, *DHCP Relay Agent Information Option (Option 82)*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3596, *DNS Extensions to Support IP version 6*

RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*

RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

RFC 4251, *The Secure Shell (SSH) Protocol Architecture*
RFC 4252, *The Secure Shell (SSH) Authentication Protocol* (publickey, password)
RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*
RFC 4254, *The Secure Shell (SSH) Connection Protocol*
RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*
RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*
RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer (ECDSA)*
RFC 5880, *Bidirectional Forwarding Detection (BFD)*
RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*
RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*
RFC 6398, *IP Router Alert Considerations and Usage (MLD)*
RFC 6528, *Defending against Sequence Number Attacks*
RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*
RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast*
draft-dolganow-bess-mvpn-expl-track-01, *Explicit Tracking with Wild Card Routes in Multicast VPN*
draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*
draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*
RFC 1112, *Host Extensions for IP Multicasting*
RFC 2236, *Internet Group Management Protocol, Version 2*
RFC 2375, *IPv6 Multicast Address Assignments*
RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*
RFC 3376, *Internet Group Management Protocol, Version 3*
RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

-
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- 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) (auto-RP groups)*
- RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*
- RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*
- RFC 4607, *Source-Specific Multicast for IP*
- RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*
- RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*
- RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
- RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*
- RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*
- RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*
- RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*
- RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*
- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*
- RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*
- RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*
- RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*
- RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*
- RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*
- RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

Internet Protocol (IP) — Version 4

RFC 791, *Internet Protocol*
RFC 792, *Internet Control Message Protocol*
RFC 826, *An Ethernet Address Resolution Protocol*
RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
RFC 1812, *Requirements for IPv4 Routers*
RFC 1918, *Address Allocation for Private Internets*
RFC 1981, *Path MTU Discovery for IP version 6*
RFC 2003, *IP Encapsulation within IP*
RFC 2401, *Security Architecture for Internet Protocol*
RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

Internet Protocol (IP) — Version 6

RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
RFC 2473, *Generic Packet Tunneling in IPv6 Specification*
RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*
RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*
RFC 3587, *IPv6 Global Unicast Address Format*
RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*
RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*
RFC 3971, *SEcure Neighbor Discovery (SEND)*
RFC 3972, *Cryptographically Generated Addresses (CGA)*
RFC 4007, *IPv6 Scoped Address Architecture*
RFC 4193, *Unique Local IPv6 Unicast Addresses*
RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*
RFC 4862, *IPv6 Stateless Address Autoconfiguration (router functions)*
RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*
RFC 5007, *DHCPv6 Leasequery*

RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*
RFC 5952, *A Recommendation for IPv6 Address Text Representation*
RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*
RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*

Internet Protocol Security (IPsec)

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*
draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*
RFC 2401, *Security Architecture for the Internet Protocol*
RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
RFC 2406, *IP Encapsulating Security Payload (ESP)*
RFC 2409, *The Internet Key Exchange (IKE)*
RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*
RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*
RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
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 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 4301, *Security Architecture for the Internet Protocol*
RFC 4303, *IP Encapsulating Security Payload*
RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
RFC 4308, *Cryptographic Suites for IPsec*
RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*

RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*
RFC 4891, *Using IPsec to Secure IPv6-in-IPv4 Tunnels*
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 5998, *An Extension for EAP-Only Authentication in IKEv2*
RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

Label Distribution Protocol (LDP)

draft-ietf-mpls-ldp-ip-pw-capability-09, *Controlling State Advertisements Of Non-negotiated LDP Applications*
draft-ietf-mpls-ldp-ipv6-15, *Updates to LDP for IPv6*
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, *Upstream LSR Redundancy for Multipoint LDP Tunnels*
draft-pdutta-mpls-multi-ldp-instance-00, *Multiple LDP Instances*
draft-pdutta-mpls-tldp-hello-reduce-04, *Targeted LDP Hello Reduction*
RFC 3037, *LDP Applicability*
RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol (helper mode)*
RFC 5036, *LDP Specification*
RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*
RFC 5443, *LDP IGP Synchronization*
RFC 5561, *LDP Capabilities*
RFC 5919, *Signaling LDP Label Advertisement Completion*
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 6826, *Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

draft-mammoliti-l2tp-accessline-avp-04, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*
RFC 2661, *Layer Two Tunneling Protocol "L2TP"*
RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*
RFC 3438, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*
RFC 3931, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*
RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*
RFC 4719, *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*
RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

Management

draft-ietf-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*
draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*
draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*
draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*
draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*
draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*
ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*
ianagmplstc-mib, *IANA-GMPLS-TC-MIB*
ianaiftype-mib, *IANAifType-MIB*
ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*
IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*
IEEE8021-PAE-MIB, *IEEE 802.1X MIB*
IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*
LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*
RFC 1157, *A Simple Network Management Protocol (SNMP)*
RFC 1212, *Concise MIB Definitions*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1215, *A Convention for Defining Traps for use with the SNMP*

RFC 1724, *RIP Version 2 MIB Extension*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

RFC 2206, *RSVP Management Information Base using SMIv2*

RFC 2213, *Integrated Services Management Information Base using SMIv2*

RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*

RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*

RFC 2515, *Definitions of Managed Objects for ATM Management*

RFC 2570, *SNMP Version 3 Framework*

RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 2573, *SNMP Applications*

RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3164, *The BSD syslog Protocol*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4)*

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

RFC 4220, *Traffic Engineering Link Management Information Base*

RFC 4273, *Definitions of Managed Objects for BGP-4*

RFC 4292, *IP Forwarding Table MIB*

RFC 4293, *Management Information Base for the Internet Protocol (IP)*

RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*

RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms (TLS)*

RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*

RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*

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*
RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* (TLS client, RSA public key)
RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)* (server, unauthenticated mode)
RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*
RFC 6020, *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*
RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*
RFC 6241, *Network Configuration Protocol (NETCONF)*
RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*
RFC 6243, *With-defaults Capability for NETCONF*
RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*
RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*
RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*
SFLOW-MIB, *sFlow MIB Version 1.3 (Draft 5)*

Multiprotocol Label Switching - Transport Profile (MPLS-TP)

RFC 5586, *MPLS Generic Associated Channel*
RFC 5921, *A Framework for MPLS in Transport Networks*
RFC 5960, *MPLS Transport Profile Data Plane Architecture*
RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*
RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*
RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*
RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*
RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*
RFC 6478, *Pseudowire Status for Static Pseudowires*
RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

Multiprotocol Label Switching (MPLS)

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

Network Address Translation (NAT)

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

Open Shortest Path First (OSPF)

draft-ietf-ospf-prefix-link-attr-06, *OSPFv2 Prefix/Link Attribute Advertisement*

draft-ietf-ospf-segment-routing-extensions-04, *OSPF Extensions for Segment Routing*

RFC 1586, *Guidelines for Running OSPF Over Frame Relay Networks*

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*

RFC 3509, *Alternative Implementations of OSPF Area Border Routers*

RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart (helper mode)*
RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*
RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*
RFC 4552, *Authentication/Confidentiality for OSPFv3*
RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
RFC 4970, *Extensions to OSPF for Advertising Optional Router Capabilities*
RFC 5185, *OSPF Multi-Area Adjacency*
RFC 5187, *OSPFv3 Graceful Restart (helper mode)*
RFC 5243, *OSPF Database Exchange Summary List Optimization*
RFC 5250, *The OSPF Opaque LSA Option*
RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
RFC 5340, *OSPF for IPv6*
RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*
RFC 5838, *Support of Address Families in OSPFv3*
RFC 6987, *OSPF Stub Router Advertisement*

OpenFlow

ONF *OpenFlow Switch Specification Version 1.3.1* (OpenFlow-hybrid switches)

Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*
draft-ietf-pce-segment-routing-05, *PCEP Extensions for Segment Routing*
draft-ietf-pce-stateful-pce-11, *PCEP Extensions for Stateful PCE*
RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*
RFC 1661, *The Point-to-Point Protocol (PPP)*
RFC 1662, *PPP in HDLC-like Framing*

RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1989, *PPP Link Quality Monitoring*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 2153, *PPP Vendor Extensions*
RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 2615, *PPP over SONET/SDH*
RFC 2686, *The Multi-Class Extension to Multi-Link PPP*
RFC 2878, *PPP Bridging Control Protocol (BCP)*
RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*
RFC 5072, *IP Version 6 over PPP*

Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points (Gx support as it applies to wireline environment (BNG))*
RFC 3588, *Diameter Base Protocol*
RFC 4006, *Diameter Credit-Control Application*

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*
MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*
MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*
MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*
MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*
RFC 3916, *Requirements for Pseudo- Wire Emulation Edge-to-Edge (PWE3)*
RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*
RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*
RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (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 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*

RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over 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 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*

RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*

RFC 6073, *Segmented Pseudowire*

RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*

RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*

RFC 6718, *Pseudowire Redundancy*

RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2598, *An Expedited Forwarding PHB*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3260, *New Terminology and Clarifications for Diffserv*

Resource Reservation Protocol - Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

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, *RSVP-TE: Extensions to RSVP for LSP Tunnels*
RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling
Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions
(IF_ID RSVP_HOP object with unnumbered interfaces and RSVP-TE graceful
restart helper procedures)*
RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic
Engineering (RSVP-TE)*
RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic
Engineering*
RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic
Engineering Tunnels*
RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*
RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic
Engineering*
RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware
MPLS Traffic Engineering*
RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS
Traffic Engineering*
RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*
RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering
(RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*
RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*
RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource
Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*
RFC 5712, *MPLS Traffic Engineering Soft Preemption*
RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering
Networks*

Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*
RFC 2080, *RIPng for IPv6*
RFC 2082, *RIP-2 MD5 Authentication*
RFC 2453, *RIP Version 2*

Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)

ITU-G.841, *Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002*

Timing

GR-1244-CORE, *Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005*

GR-253-CORE, *SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions, issued 09/2008*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003*

ITU-T G.8261, *Timing and synchronization aspects in packet networks, issued 04/2008*

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007*

ITU-T G.8264, *Distribution of timing information through packet networks, issued 10/2008*

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization, issued 10/2010*

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

Virtual Private LAN Service (VPLS)

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550 Appendix A.8, *RTP: A Transport Protocol for Real-Time Applications* (estimating the interarrival jitter)

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses (S2a roaming based on GPRS)*

Customer Document and Product Support



Customer Documentation

[Customer Documentation Welcome Page](#)



Technical Support

[Product Support Portal](#)



Documentation Feedback

[Customer Documentation Feedback](#)

