



7210 SAS D, E OS Basic System Configuration Guide

Software Versions: 7210 SAS OS 6.0 Rev.01

July 2013

Document Part Number: 93-0493-01-01



This document is protected by copyright. Except as specifically permitted herein, no portion of the provided information can be reproduced in any form, or by any means, without prior written permission from Alcatel-Lucent.
Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.
The information presented is subject to change without notice.
Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright 2013 Alcatel-Lucent. All rights reserved.

TABLE OF CONTENTS

Preface	11
Getting Started	
Alcatel-Lucent 7210 SAS-Series System Configuration Process	15
CLI Usage	
CLI Structure	18
Navigating in the CLI	20
CLI Contexts	20
Basic CLI Commands	22
CLI Environment Commands	25
CLI Monitor Commands	26
Getting Help in the CLI	27
The CLI Command Prompt	29
Displaying Configuration Contexts	30
EXEC Files	33
Entering CLI Commands	34
Command Completion	34
Unordered Parameters	34
Editing Keystrokes	35
Absolute Paths	36
History	38
Entering Numerical Ranges	39
Pipe/Match	41
Redirection	44
Basic Command Reference	45
File System Management	
The File System	82
Compact Flash Devices	82
USB Storage Device	83
URLs	84
Wildcards	86
File Management Tasks	87
Creating Directories	88
Copying Files	89
Moving Files	90
Removing Files and Deleting Directories	90
Displaying Directory and File Information	91
File Command Reference	93
Boot Options	
System Initialization	108
Manual Mode	111
.....	112

Table of Contents

Auto Init	112
Configuration Guidelines for use of Auto-init and Manual mode	112
Configuration and Image Loading	114
Ping Check	118
Persistence	119
Configuration guidelines for use of software images with the 128MB 7210 SAS-D platform	121
Out-of-band (OOB) Ethernet Management Port	121
Configuration Guidelines for use of IPv6 for out-of-band management of the node	121
Security for Console Port and Ethernet Management Port	122
Reset the node to factory default setting	122
Initial System Startup Process Flow	126
Configuration Notes	127
Configuring Boot File Options with CLI	129
BOF Configuration Overview	130
Basic BOF Configuration	131
Common Configuration Tasks	133
Searching for the BOF	134
Accessing the CLI	137
Console Connection	137
Configuring BOF Parameters	139
Service Management Tasks	140
System Administration Commands	140
Viewing the Current Configuration	140
Modifying and Saving a Configuration	142
Deleting BOF Parameters	143
Saving a Configuration to a Different Filename	145
Rebooting	145
BOF Command Reference	147

System Management

System Management Parameters	174
System Information	174
System Name	174
System Contact	174
System Location	175
System Coordinates	175
Naming Objects	175
Common Language Location Identifier	176
System Time	177
Time Zones	177
Network Time Protocol (NTP)	179
SNTP Time Synchronization	180
CRON	181
High Availability	182
HA Features	182
Redundancy	182
Temperature Threshold Alarm and Fan Speed	184
Synchronization	186
Line Timing Mode	186

Synchronous Ethernet	186
Network Synchronization	187
Central Synchronization Sub-System	188
Synchronization Status Messages (SSM)	190
IEEE 1588v2 PTP	191
PTP Clock Synchronization	195
Performance Considerations	198
PTP Capabilities	198
PTP Ordinary Slave Clock For Frequency	199
PTP Boundary Clock for Frequency and Time	199
Configuration guidelines for PTP on 7210 SAS-DETR	200
Configuration to change reference from syncE to PTP	201
Management of 1830 VWM	203
Introduction to 1830 VWM CWDM Passive Optical device	203
Feature Description	204
Configuration Guidelines	205
Link Layer Discovery Protocol (LLDP)	206
System Configuration Process Overview	209
Configuration Notes	210
General	210
Configuring System Management with CLI	211
System Management	212
Saving Configurations	212
Basic System Configuration	213
Common Configuration Tasks	214
System Information	215
System Information Parameters	216
Coordinates	218
System Time Elements	219
Configuring Backup Copies	240
System Administration Parameters	241
Validating the Golden Bootstrap Image	241
Updating the Golden Bootstrap Image	242
Disconnect	242
Set-time	243
Display-config	243
Tech-support	245
Save	245
Reboot	246
Post-Boot Configuration Extension Files	247
System Timing	250
Edit Mode	250
Configuring Timing References	251
Using the Revert Command	252
Configuring System Monitoring Thresholds	253
Creating Events	253
System Alarm Contact Inputs in 7210 SAS-E devices	255
Configuring LLDP	256
System Resource Allocation	257

Table of Contents

Allocation of Ingress Internal TCAM resources257

Allocation of Egress Internal TCAM resources258

System Resource Allocation Examples259

Standards and Protocol Support (7210 SAS-D)409

Standards and Protocol Support (7210 SAS E).....413

Index415

LIST OF TABLES

Getting Started

Table 1:	Configuration Process	15
----------	---------------------------------	----

CLI Usage

Table 2:	Console Control Commands	22
Table 3:	Command Syntax Symbols	24
Table 4:	CLI Environment Commands	25
Table 5:	CLI Monitor Command Contexts	26
Table 6:	Online Help Commands	27
Table 7:	Command Editing Keystrokes	35
Table 8:	CLI Range Use Limitations	39
Table 9:	Regular Expression Symbols	42
Table 10:	Special Characters	43
Table 11:	Show Alias Output Fields	80

File System Management

Table 12:	URL types and Syntax	84
Table 13:	File Command Local and Remote File System Support	86

Boot Options

Table 14:	Console Configuration Parameter Values	137
Table 15:	Show BOF Output Fields	167
Table 16:	Show BOF Output Fields (supported only on 7210 SAS-E)	168

System Management

Table 17:	System-defined Time Zones	177
Table 18:	Temperature Thresholds for 7210 SAS-D Devices	185
Table 19:	Revertive, non-Revertive Timing Reference Switching Operation	189
Table 20:	Local Clock Parameters When Profile is set to ieee1588-2008	193
Table 21:	Local Clock Parameters When Profile is set to: itu-telecom-freq	194
Table 22:	Support Message Rates for Slave and Master Clock States	198
Table 23:	System-defined Time Zones	220
Table 24:	Values and the corresponding pps rate	297
Table 25:	Show System CPU Output Fields	363
Table 26:	Show Memory Pool Output Fields	373
Table 27:	Show system resource-profile output fields	378
Table 28:	Show System SNTP Output Fields	382
Table 29:	Show System Time Output Fields	386
Table 30:	Show VWM-shelf Output Fields	387
Table 31:	Show System tod-suite Output Fields	389
Table 32:	Show System Time-range Output Fields	392
Table 33:	System Timing Output Fields	393

LIST OF FIGURES

CLI Usage

Figure 1:	Root Commands	18
Figure 2:	Operational Root Commands	19

File System Management

Boot Options

Figure 3:	Bootstrap Load Process - System Initialisation - Part I	109
Figure 4:	Files on the Flash	110
Figure 5:	Bootstrap Process - System Initialization - Part II-A	115
Figure 6:	Bootstrap Process - System Initialization - Part II-B	116
Figure 7:	Bootstrap Process - System Initialization - Part II-C	117
Figure 8:	Timos Boot - System Initialization - Part III	118
Figure 9:	System Startup Process Flow	126
Figure 10:	7210 SAS E Front Panel Console Port	138
Figure 11:	7210 SAS D Front Panel Console Port	138

System Management

Figure 12:	Conventional Network Timing Architecture (North American Nomenclature)	187
Figure 13:	Synchronization Reference Selection	188
Figure 14:	Peer Clocks	192
Figure 15:	Messaging Sequence Between the PTP Slave Clock and PTP Master Clocks	195
Figure 16:	PTP Slave Clock and Master Clock Synchronization Timing Computation	196
Figure 17:	Using IEEE 1588v2 For Time Distribution	197
Figure 18:	Slave Clock	199
Figure 19:	Boundary Clock	200
Figure 20:	Optical Ring with 7210 SAS and 1830 VWM Passive Optical unit	203
Figure 21:	LLDP Internal Architecture for a Network Node	207
Figure 22:	Customer Use Example For LLDP	208
Figure 23:	System Configuration and Implementation Flow	209

About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure 7210 SAS-Series boot option file (BOF), file system and system management functions.

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

Audience

This manual is intended for network administrators who are responsible for configuring the 7210 SAS-Series routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and processes described in this manual 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 CLI code, time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), and synchronization properties

List of Technical Publications

The 7210-SAS D, E OS documentation set is composed of the following books:

- 7210-SAS D, E OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7210-SAS D, E OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7210-SAS D, E OS Interface Configuration Guide
This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- 7210-SAS D, E OS Router Configuration Guide
This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP-based filtering.
- 7210-SAS D, E OS Routing Protocols Guide
This guide provides an overview of routing concepts and provides configuration examples for protocols and route policies.
- 7210-SAS D, E OS Services Guide
This guide describes how to configure service parameters such as customer information, and user services.
- 7210-SAS D, E OS OAM and Diagnostic Guide
This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- 7210-SAS D, E OS Quality of Service Guide
This guide describes how to configure Quality of Service (QoS) policy management.

Technical Support

If you purchased a service agreement for your 7210 SAS-Series router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center:

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml

Getting Started

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.

Alcatel-Lucent 7210 SAS-Series System Configuration Process

[Table 1](#) 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 7210 SAS-Series device configuration tasks in the following order:

Table 1: Configuration Process

Area	Task	Chapter
CLI Usage	The CLI structure	CLI Usage on page 17
	Basic CLI commands	Basic CLI Commands on page 22
	Configure environment commands	CLI Environment Commands on page 25
	Configure monitor commands	CLI Monitor Commands on page 26
Operational functions	Directory and file management	File System Management on page 81

Table 1: Configuration Process

Area	Task	Chapter (Continued)
Boot options	Configure boot option files (BOF)	Boot Options on page 107
System configuration	Configure system functions, including host name, address, domain name, and time parameters.	System Management on page 173
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 407

In This Chapter

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

Topics in this chapter include:

- [CLI Structure on page 18](#)
- [Navigating in the CLI on page 20](#)
- [Basic CLI Commands on page 22](#)
- [CLI Environment Commands on page 25](#)
- [CLI Monitor Commands on page 26](#)
- [Getting Help in the CLI on page 27](#)
- [The CLI Command Prompt on page 29](#)
- [Displaying Configuration Contexts on page 30](#)
- [EXEC Files on page 33](#)
- [Entering CLI Commands on page 34](#)

CLI Structure

Alcatel-Lucent’s Operating System (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 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.

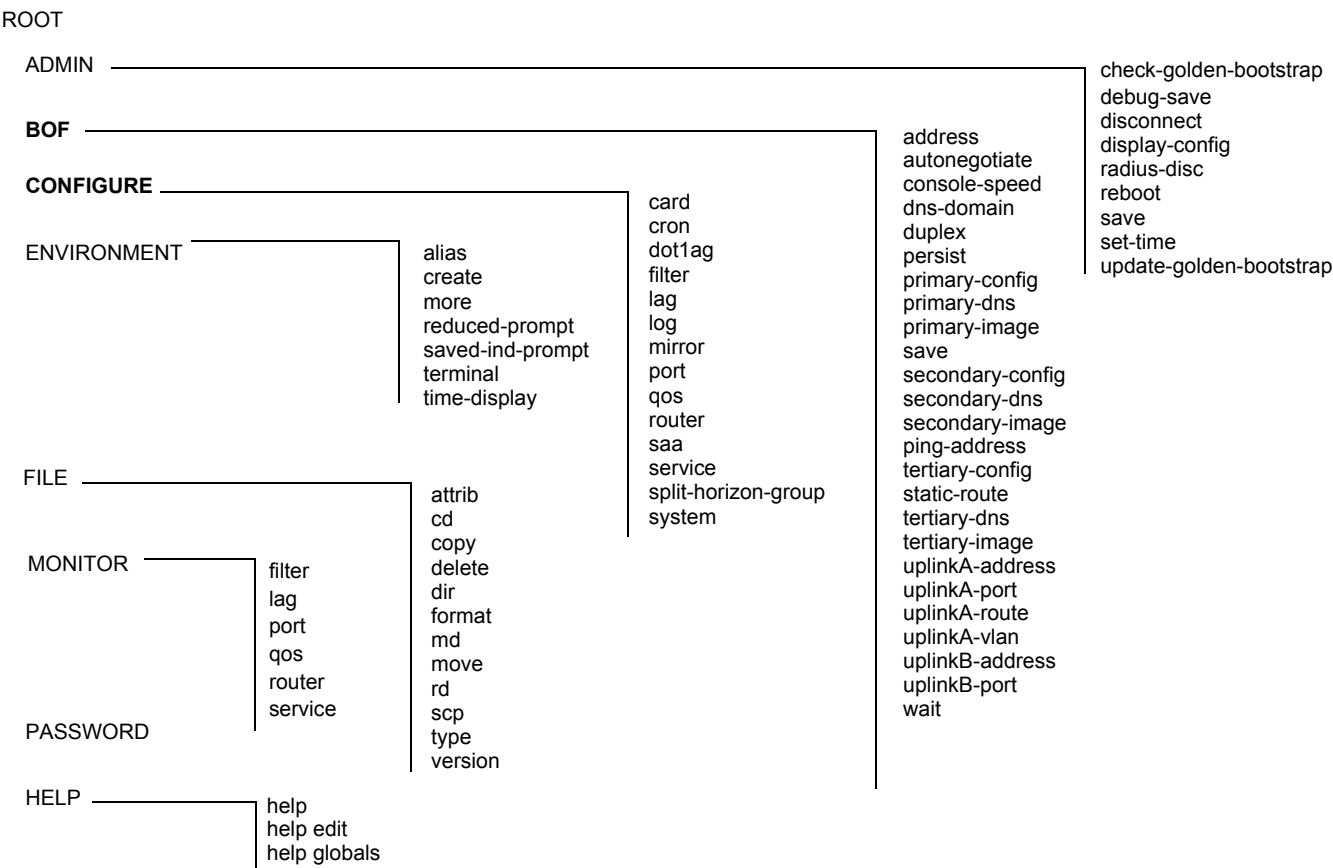


Figure 1: Root Commands

ROOT

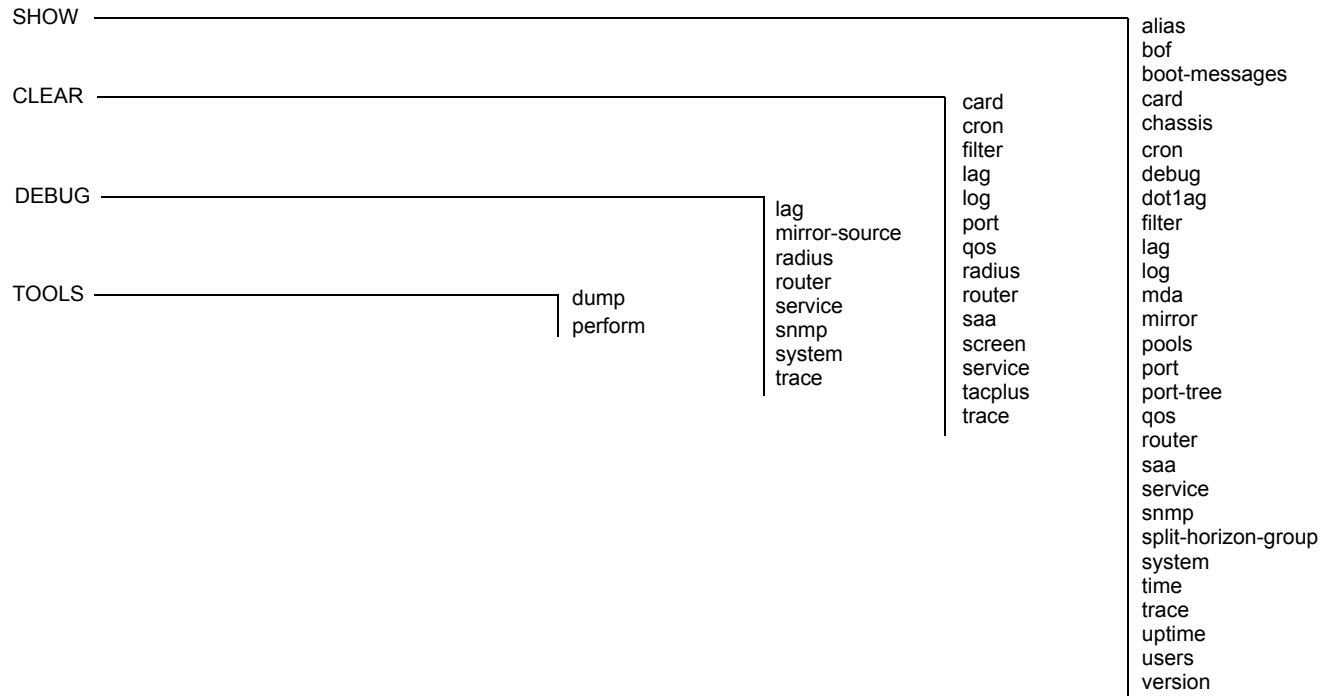


Figure 2: Operational Root Commands

Navigating in the CLI

The following sections describe additional navigational and syntax information.

- [CLI Contexts on page 20](#)
 - [Basic CLI Commands on page 22](#)
 - [CLI Environment Commands on page 25](#)
 - [CLI Monitor Commands on page 26](#)
 - [Entering Numerical Ranges on page 39](#)
-

CLI Contexts

Use the CLI to access, configure, and manage Alcatel-Lucent's 7210 SAS devices. 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:ALU-7210# config
A:ALU-7210>config#
```

In a given CLI context, you can 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 SAP ingress level:

Method 1:

```
A:ALU-7210# config service epipe 6 sap 1/1/2 ingress
```

Method 2:

```
A:ALU-7210# configure
A:ALU-7210>config# service
A:ALU-7210>config>service# epipe 6
A:ALU-7210>config>service>epipe# sap 1/1/2
A:ALU-7210>config>service>epipe>sap# ingress
A:ALU-7210>config>service>epipe>sap>ingress#
```

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

```
A:ALU-7210>config>service>epipe# sapp
      ^
Error: Bad command.
A:ALU-7210>config>service>epipe#
```

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 2](#).

Table 2: Console Control Commands

Command	Description	Page
<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.	50
clear	Clears statistics for a specified entity or clears and resets the entity.	50
echo	Echos the text that is typed in. Primary use is to display messages to the screen within an exec file.	51
exec	Executes the contents of a text file as if they were CLI commands entered at the console.	51
exit	Returns the user to the previous higher context.	51
exit all	Returns the user to the ROOT context.	52
help ?	Displays help in the CLI.	52
history	Displays a list of the most recently entered commands.	54
info	Displays the running configuration for a configuration context.	54
logout	Terminates the CLI session.	58
oam	Provides OAM test suite options. See the OAM section of the 7210 SAS OS OAM and Diagnostic Guide.	
password	Changes the user CLI login password. The password can only be changed at the ROOT level.	59
ping	Verifies the reachability of a remote host.	59
pwc	Displays the present or previous working context of the CLI session.	61

Table 2: Console Control Commands (Continued)

Command	Description	Page
<code>sleep</code>	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.	62
<code>ssh</code>	Opens a secure shell connection to a host.	62
<code>telnet</code>	Telnet to a host.	62
<code>traceroute</code>	Determines the route to a destination address.	63
<code>tree</code>	Displays a list of all commands at the current level and all sublevels.	64
<code>write</code>	Sends a console message to a specific user or to all users with active console sessions.	64

The list of all system global commands is displayed by entering `help globals` in the CLI. For example:

```
A:ALU-7210>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
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:ALU-7210>config>service#
```

[Table 3](#) lists describes command syntax symbols.

Table 3: 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}
[]	Brackets indicate optional parameters. redirects [number seconds]
< >	Angle brackets indicate that you must enter text based on the parameter inside the brackets. interface <interface-name>
{ }	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. • sdp <i>sdp-id</i> [{gre mpls}] vpls <i>service-id</i> [svc-sap-type {null-star dot1q dot1q-preserve}]
Bold	Commands in bold indicate commands and keywords.
<i>Italic</i>	Commands in <i>italics</i> indicate command options.

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 4](#).

Table 4: CLI Environment Commands

Command	Description	Page
alias	Enables the substitution of a command line by an alias.	65
create	Enables or disables the use of a create parameter check.	65
more	Configures whether CLI output should be displayed one screen at a time awaiting user input to continue.	65
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.	66
saved-ind-prompt	Saves the indicator in the prompt.	66
terminal	Configures the terminal screen length for the current CLI session.	67
time-display	Specifies whether time should be displayed in local time or UTC.	67

CLI Monitor Commands

Monitor commands display specified statistical information related to the monitor subject (such as filter, port, QoS, router, service) 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 4](#).

Table 5: CLI Monitor Command Contexts

Command	Description	Page
filter	Enables IP, IPv6 and MAC filter monitoring at a configurable interval until that count is reached.	68
lag	Enables Link Aggregation Group (LAG) monitoring to display statistics for individual port members and the LAG.	72
port	Enables port traffic monitoring. The specified port(s) statistical information displays at the configured interval until the configured count is reached.	75
service	Monitors commands for a particular service.	77

Getting Help in the CLI

The **help** system commands and the `?` key display different types of help in the CLI. [Table 6](#) lists the different help commands.

Table 6: Online Help Commands

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

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

The following example displays a partial list of the `tree` and `tree detail` command output entered at the `config` level.

Getting Help in the CLI

A:ALU-7210>config# tree

```
configure
+---card
|   +---card-type
|   +---mda
|       +---access
|       +---mda-type
|       +---network
|       +---shutdown
|   +---shutdown
+---cron
|   +---action
|       +---expire-time
|       +---lifetime
|       +---max-completed
|       +---results
|       +---script
|       +---shutdown
|   +---schedule
|       +---action
|       +---count
|       +---day-of-month
|       +---description
|       +---end-time
|       +---hour
|       +---interval
|       +---minute
|       +---month
|       +---shutdown
|       +---type
|       +---weekday
|   +---script
|       +---description
|       +---location
|       +---shutdown
|   +---time-range
|       +---absolute
|       +---daily
|       +---description
|       +---weekdays
|       +---weekend
|       +---weekly
|   +---tod-suite
|       +---description
|       +---egress
|       |   +---filter
|       |   +---qos
|       |   +---scheduler-policy
|       +---ingress
|       |   +---filter
|       |   +---qos
|       |   +---scheduler-policy
+---dot1ag
|   +---domain
|   +---association
```

*A:ALA-12>config# tree detail

```
configure
+---card <slot-number>
|   no card <slot-number>
|   +---card-type <card-type>
|       no card-type
|   +---mda <mda-slot>
|       no mda <mda-slot>
|       +---access
|       +---mda-type <mda-type>
|           no mda-type
|       +---network
|       +---no shutdown
|           shutdown
|   +---no shutdown
|       shutdown
+---cron
|   +---action <action-name> [owner <action-owner>]
|       no action <action-name> [owner <action-owner>]
|       +---expire-time {<seconds>|forever}
|       +---lifetime {<seconds>|forever}
|       +---max-completed <unsigned>
|       +---no results
|           results <file-url>
|       +---no script
|           script <script-name> [owner <script-owner>]
|       +---no shutdown
|           shutdown
|   +---no schedule <schedule-name> [owner <schedule-owner>]
|       schedule <schedule-name> [owner <schedule-owner>]
|       +---action <action-name> [owner <action-owner>]
|           no action
|       +---count <number>
|           no count
|       +---day-of-month {<day-number> [..<day-number>]]all}
|           no day-of-month
|       +---description <description-string>
|           no description
|       +---end-time [<date>|<day-name>] <time>
|           no end-time
|       +---hour {<hour-number> [..<hour-number>]]all}
|           no hour
|       +---interval <seconds>
|           no interval
|       +---minute {<minute-number> [..<minute-number>]]all}
|           no minute
|           +---month {<month-number> [..<month-number>]]<month-name>
|               [..<month-nam>]]all}
|           no month
|       +---no shutdown
|           shutdown
|       +---type <schedule-type>
|           +---weekday {<weekday-number> [..<weekday-number>]]<day-name>
|               [..<day-nme>]]all}
|   ...
```

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:ALU-7210>config>router# interface "primary#1"
```

When changes are made to the configuration file a "*" appears in the prompt string (*A:ALU-7210) 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.

Displaying Configuration Contexts

The **info** and **info detail** commands display configuration for the current level. The **info** command displays non-default configurations. The **info detail** command displays the entire configuration for the current level, including defaults. The following example shows the output that displays using the **info** command and the output that displays using the **info detail** command.

```
*A:ALA>config>service>vpls# info
-----
      stp
        shutdown
      exit
      sap 1/1/14:100 create
      exit
      sap 1/1/15:100 create
      exit
      no shutdown
-----

*A:ALA>config>service>vpls# info detail
-----
      no description
      no disable-learning
      no disable-aging
      no discard-unknown
      fdb-table-size 250
      fdb-table-high-wmark 95
      fdb-table-low-wmark 90
      local-age 300
      stp
        shutdown
        priority 32768
        hello-time 2
        forward-delay 15
        max-age 20
        hold-count 6
        mode rstp
      exit
      mac-move
        move-frequency 2
        retry-timeout 10
        shutdown
      exit
      sap 1/1/14:100 create
        no description
        no tod-suite
        limit-mac-move blockable
        no disable-aging
        no max-nbr-mac-addr
        no discard-unknown-source
        no mac-pinning
        stp
          path-cost 10
          priority 128
          no edge-port
          auto-edge
```

```

        link-type pt-pt
        no root-guard
        no shutdown
    exit
    dotlag
    exit
    no authentication-policy
    no l2pt-termination
    no bpdu-translation
    ingress
        qos 1
        no match-qinq-dotlp
        no filter
    exit
    egress
        no qinq-mark-top-only
        no filter
        no agg-rate-limit
    exit
    no collect-stats
    no accounting-policy
    no shutdown
exit
sap 1/1/15:100 create
    no description
    no tod-suite
    limit-mac-move blockable
    no disable-aging
    no max-nbr-mac-addr
    no discard-unknown-source
    no mac-pinning
    stp
        path-cost 10
        priority 128
        no edge-port
        auto-edge
        link-type pt-pt
        no root-guard
        no shutdown
    exit
    dotlag
    exit
    no authentication-policy
    no l2pt-termination
    no bpdu-translation
    ingress
        qos 1
        no match-qinq-dotlp
        no filter
    exit
    egress
        no qinq-mark-top-only
        no filter
        no agg-rate-limit
    exit
    no collect-stats
    no accounting-policy
    no shutdown
exit

```

```
no shutdown
-----
*A:ALA>config>service>vpls#
```


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.

Entering CLI Commands

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.

Unordered 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-1>config>router# static-route
- [no] static-route {<ip-prefix/prefix-length>|<ip-prefix> <netmask>}
  [preference <preference>] [metric <metric>] [enable|disable] next-hop
  <gateway>
- [no] static-route {<ip-prefix/prefix-length>|<ip-prefix> <netmask>}
  [preference <preference>] [metric <metric>] [enable|disable] black-hole
```

Editing Keystrokes

When entering a command, special keystrokes allow for editing of the command. [Table 7](#) lists the command editing keystrokes.

Table 7: 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>

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 forward slash “/” or backward slash “\” cannot be used with the **environment alias** command. The commands are interpreted as absolute path. 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#
```

Note that 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),

CLI Syntax: config>service>ies> /clear card 1

behaves the same as the following series of commands.

Example: 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:

CLI Syntax: `config>service>ies>/configure service ies 5 create`

becomes

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

History

The CLI maintains a history of the most recently entered commands. The **history** command displays 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 1/1/1
 8 con port 1/1/1
 9 \con port 1/1/1
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:cses-E11# show version
TiMOS-B-0.0.I2838 both/i386 ALCATEL SR 7750 Copyright (c) 2000-2011 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Mon Jan 10 18:33:16 PST 2011 by builder in /rel0.0/I2838/panos/main
A:cses-E11#
TiMOS-B-0.0.I232 both/i386 ALCATEL SAS-E 7210 Copyright (c) 2000-2008 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Sat Oct 11 18:15:40 IST 2008 by panosbld in /panosbld/ws/panos/main
*A:ALU-7210#
```

Entering Numerical Ranges

The 7210-SAS OS CLI allows the use of a single numerical range as an argument in the command line. A range in a CLI command is limited to positive integers and is denoted with two numbers enclosed in square brackets with two periods (“..”) between the numbers:

$$[x..y]$$

where x and y are positive integers and $y-x$ is less than 1000.

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

Specifying a range in the CLI does have limitations. These limitations are summarized in [Table 8](#).

Table 8: CLI Range Use Limitations

Limitation	Description
Only a single range can be specified.	It is not possible to shut down ports 1 through 10 on MDA 1 and MDA 2, as the command would look like <pre>configure port 1/[1..2]/[1..10]</pre> and requires two ranges in the command, [1..2] for the MDA and [1..10] for the port number.
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, <pre>configure router interface "A[1..10]" no shutdown</pre> creates a single router interface with the name “A[1..10]”. However, a command such as: <pre>configure router interface A[1..10] no shutdown</pre> creates 10 interfaces with names A1, A2 .. A10.

Table 8: CLI Range Use Limitations (Continued)

Limitation	Description
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, <code>configure port 1/1/[1..10]</code> 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 may 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, may cease to work. If the command line entered is correct and unambiguous, the command works properly; otherwise, an error is returned.

Pipe/Match

The 7210-SAS OS supports the pipe feature to search one or more files for a given character string or pattern.

Note: When using the pipe/match command the variables and attributes must be spelled correctly. The attributes following the command and must come before the expression/pattern. The following displays examples of 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” > cf3cfl:\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

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:

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

For example:

```
*A:Dut-G# show log log-id 99 | match ignore-case sap
"Processing of an access port state change event is finished and the status of all affected
SAPs on port 1/1/21 has been updated."
"Service Id 4001, SAP Id 1/1/21:0.* configuration modified"

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, operational
state: up"

*A:Dut-G# admin display-config | match post-lines 4 max-count 2 expression "vpls"
#-----
...
    vpls 1 customer 1 svc-sap-type null-star create
        description "Default tls description for service id 1"
        stp
            shutdown
        exit
    vpls 2 customer 1 svc-sap-type null-star create
        description "Default tls description for service id 2"
        stp
            shutdown
        exit
...
#-----
```

[Table 9](#) describes regular expression symbols and interpretation (similar to what is used for route policy regexp matching). [Table 10](#) describes special characters.

Table 9: 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.

Table 9: Regular Expression Symbols (Continued)

String	Description
{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 10: Special Characters

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

Redirection

The 7210-SAS 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).

```
'ping <customer_ip> > cf3cf1:/ping/result.txt'  
'ping <customer_ip> > ftp://ron@ftp.alcatel.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”).

Basic Command Reference

Command Hierarchies

- [Global CLI Commands](#)
- [Environment Commands](#)
- [Monitor Commands](#)

Global CLI Commands

```

— back
— clear
— echo [text-to-echo] [extra-text-to-echo] [more-text]
— enable-admin
— exec [-echo] [-syntax] filename
— exit [all]
— help
— history
— info [detail]
— logout
— 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]][timeout time-out]
— pwc [previous]
— sleep [seconds]
— ssh [ip-addr | dns-name] [username@ip-addr] [-l username] [-v SSH-version] [router router-instance]
— 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]
— write {user | broadcast} message-string

```

Monitor Commands

```
monitor
— 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]
— port port-id [port-id...(up to 5 max)] [interval seconds] [repeat repeat] [absolute | rate]
— service
    — id service-id
        — sap sap-id [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]
```

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
    — terminal
        — length lines
    — time-display {local | utc}
    — [no] time-stamp
```

Basic CLI Commands

Global Commands

enable-admin

Syntax	enable-admin
Context	<global>
Description	NOTE: 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 is determined by the complexity command.

The following displays 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#
```

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 ospfconfig router interface <i>interface-id</i> context, the back command moves the cursor to the config router context level.

clear

Syntax	clear
Context	<GLOBAL>
Description	This command clears statistics for a specified entity or clears and resets the entity.
Parameters	cron — Clears CRON history. filter — Clears IP, MAC, and log filter counters. lag — Clears LAG-related entities. log — Closes and reinitializes the log specified by log-id. port — Clears port statistics. qos — Clears QoS statistics. radius — Clears the RADIUS server state. router — Clears router commands affecting the router instance in which they are entered. Values arp, authentication, bfd, dhcp, forwarding-table, icmp-redirect-route, interface, isis, ldp, mpls, ospf, rip, rsvp saa — Clears the SAA test results. screen — Clears the console or telnet screen. service — Clears service ID and statistical entities. system — Clears (re-enables) a previously failed reference. tacplus — Clears the TACACS+ server state. trace — Clears the trace log.

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.
Parameters	<i>text-to-echo</i> — Specifies a text string to be echoed up to 256 characters. <i>extra-text-to-echo</i> — Specifies more text to be echoed up to 256 characters. <i>more-text</i> — Specifies more text to be echoed up to 256 characters.

exec

Syntax	exec [-echo] [-syntax] { <i>filename</i> [<i>eof_string</i>]}
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.
Parameters	-echo — Echo the contents of the exec file to the session screen as it executes. Default Echo disabled. -syntax — Perform 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. <i>filename</i> — 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 “<i>eof_string</i><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. <i>eof_string</i> — 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
Related Commands	boot-bad-exec command on page 278 — Use this command to configure a URL for a CLI script to exec following a failed configuration boot. boot-good-exec command on page 278 — Use this command to configure a URL for a CLI script to exec following a successful configuration boot.

exit

Syntax	exit [all]
Context	<GLOBAL>
Description	This command returns to the context from which the current level was entered. For example, if you navigated to the current level on a context by context basis, then the exit command only moves the cursor back one level. <pre>A:Dut-G# configure A:Dut-G>config# service A:Dut-G>config>service# vpls 1 A:Dut-G>config>service>vpls# exit A:Dut-G>config>service# exit A:Dut-G>config# exit</pre> 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. <pre>A:Dut-G# configure service vpls 1 A:Dut-G>config>service>vpls# exit A:Dut-G#</pre> The exit all command moves the cursor all the way back to the root level. <pre>A:Dut-G# configure A:Dut-G>config# service A:Dut-G>config>service# vpls 1 A:Dut-G>config>service>vpls# exit all A:Dut-G#</pre>
Parameters	all — Exits back to the root CLI context.

help

Syntax	help help edit help global help special-characters <GLOBAL>
Description	This command provides a brief description of the help system. The following information displays: Help may be requested at any point by hitting a question mark '?'. In case of an executable node, the syntax for that node will be displayed with an explanation of all parameters. In case of sub-commands, a brief description is provided. Global Commands: Help on global commands can be observed by issuing "help globals" at any time. Editing Commands: Help on editing commands can be observed by issuing "help edit" at any time.
Parameters	help — Displays a brief description of the help system. help edit — Displays help on editing. Available editing keystrokes:

```

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

```

help 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> — Complete a partial command name (auto-completion) or list available commands that match the string.

history

Syntax	history
Context	<GLOBAL>
Description	This command lists the last 30 commands entered in this session. Re-execute a command in the history with the !n command, where n is the line number associated with the command in the history output. For example: <pre>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#</pre>

info

Syntax	info [detail]
Context	<GLOBAL>
Description	This command displays the running configuration for the configuration context.

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

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.

For example,

```
*A:STU-1>config>service# info detail
-----
      customer 1 create
        description "Default customer"
        no contact
        no phone
      exit
    ies 1 customer 1 create
      no description
      interface "new" create
        no description
        address 21.0.0.2/8
        no mac
        arp-timeout 14400
        icmp
          redirects 100 10
          unreachable 100 10
          ttl-expired 100 10
        exit
      sap 1/1/18:0.* create
        no description
        ingress
          no match-qinq-dot1p
          no filter
        exit
        egress
          no qinq-mark-top-only
          no filter
        exit
        no shutdown
      exit
      no shutdown
    exit
  no shutdown
exit
vpls 100 customer 1 svc-sap-type dot1q create
  no description
  no disable-learning
  no disable-aging
  no discard-unknown
  fdb-table-size 250
  fdb-table-high-wmark 95
  fdb-table-low-wmark 90
  local-age 300
  stp
    shutdown
    priority 32768
    hello-time 2
    forward-delay 15
    max-age 20
    hold-count 6
    mode rstp
```

```
exit
mac-move
    move-frequency 2
    retry-timeout 10
    shutdown
exit
sap 1/1/14:100 create
    no description
    no tod-suite
    limit-mac-move blockable
    no disable-aging
    no max-nbr-mac-addr
    no discard-unknown-source
    no mac-pinning
    stp
        path-cost 10
        priority 128
        no edge-port
        auto-edge
        link-type pt-pt
        no root-guard
        no shutdown
    exit
    dotlag
    exit
    no authentication-policy
    no l2pt-termination
    no bpdu-translation
    ingress
        qos 1
        no match-qinq-dot1p
        no filter
    exit
    egress
        no qinq-mark-top-only
        no filter
        no agg-rate-limit
    exit
    no collect-stats
    no accounting-policy
    no shutdown
exit
sap 1/1/15:100 create
    no description
    no tod-suite
    limit-mac-move blockable
    no disable-aging
    no max-nbr-mac-addr
    no discard-unknown-source
    no mac-pinning
    stp
        path-cost 10
        priority 128
        no edge-port
        auto-edge
        link-type pt-pt
        no root-guard
        no shutdown
    exit
    dotlag
    exit
```



```

no authentication-policy
no l2pt-termination
no bpdu-translation
ingress
    qos 1
    no match-qinq-dot1p
    no filter
exit
egress
    no qinq-mark-top-only
    no filter
    no agg-rate-limit
exit
no collect-stats
no accounting-policy
no shutdown
exit
no shutdown
exit
ies 4001 customer 1 create
no description
interface "inband" create
no description
address 192.168.1.11/24
no mac
arp-timeout 14400
icmp
    redirects 100 10
    unreachableables 100 10
    ttl-expired 100 10
exit
sap 1/1/24:0.* create
no description
ingress
    no match-qinq-dot1p
    no filter
exit
egress
    no qinq-mark-top-only
    no filter
exit
no shutdown
exit
no shutdown
exit
interface "direct" create
no description
address 10.135.16.97/24
no mac
arp-timeout 14400
icmp
    redirects 100 10
    unreachableables 100 10
    ttl-expired 100 10
exit
sap 1/1/21:0.* create
no description
ingress
    no match-qinq-dot1p
    no filter
exit

```

```
        egress
        no qinq-mark-top-only
        no filter
    exit
    no shutdown
exit
no shutdown
exit
no shutdown
exit
-----
*A:STU-1>config>service#
```

Parameters **detail** — Displays all configuration parameters including parameters at their default values.

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.

password

Syntax	password
Context	<ROOT>
Description	This command changes a user CLI login password. When a user logs in after the administrator forces a new-password-at-login, or the password has expired (aging), then this command is automatically invoked. When invoked, the user is prompted to enter the old password, the new password, and then the new password again to verify the correct input. If a user fails to create a new password after the administrator forces a new-password-at-login or after the password has expired, the user is not allowed access to the CLI.

ping

Syntax	ping { <i>ip-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 to verify IP reachability.
Parameters	<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. Values ipv4-address - a.b.c.d ipv6-address - x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d x: 0 — FFFF H d: 0 — 255 D rapid detail — The rapid parameter specifies to send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the count option.

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

Example output:

```
*A:ALU-7210# ping 192.xxx.xxx.xxx
PING 192.xxx.xxx.xxx 56 data bytes
64 bytes from 192.xxx.xxx.xxx: icmp_seq=1 ttl=64 time<10ms.
64 bytes from 1192.xxx.xxx.xxx: icmp_seq=2 ttl=64 time<10ms.
64 bytes from 192.xxx.xxx.xxx: icmp_seq=3 ttl=64 time<10ms.
```

```
64 bytes from 192.xxx.xxx.xxx: icmp_seq=4 ttl=64 time<10ms.
64 bytes from 192.xxx.xxx.xxx: icmp_seq=5 ttl=64 time<10ms.

---- 192.xxx.xxx.xxx PING Statistics ----
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min < 10ms, avg < 10ms, max < 10ms, stddev < 10ms
*A:ALU-7210#
```

ttl *time-to-live* — The IP Time To Live (TTL) value to include in the ping request, expressed as a decimal integer.

Values 0 — 128

tos *type-of-service* — The type-of-service (TOS) bits in the IP header of the ping packets, expressed as a decimal integer.

Values 0 — 255

size *bytes* — The size in bytes of the ping request packets.

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

Values 0 — 65507

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

Values 0 — 65535

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

Default The IP address of the egress IP interface.

Values *ipv4-address* - a.b.c.d
ipv6-address - x:x:x:x:x:x:x:x[-interface]
 x:x:x:x:x:x:x:x[-interface]
 x:x:x:x:x:d.d.d.d
 x: 0 — FFFF H
 d: 0 — 255 D

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

Default 1

Values 1 — 10000

next-hop *ip-address* — This option 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.

Default Per the routing table.

Values *ipv4-address* - a.b.c.d
ipv6-address - x:x:x:x:x:x:x:x[-interface]
 x:x:x:x:x:d.d.d.d[-interface]
 x - [0..FFFF]H
 d - [0..255]D

interface *interface-name* — Specify the interface name.

- bypass-routing** — Send 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.
- Default** 5
- Values** 1 — 10000
- do-not-fragment** — Specifies that the request frame should not be fragmented. This option is particularly useful in combination with the size parameter for maximum MTU determination.
- router** *router-instance* — Specify the router name or service ID.
- Default** Base
- Values** *router-name:* Base, management
service-id: 1 — 2147483647
- timeout** *timeout* — Specify the timeout in seconds.
- Default** 5
- Values** 1 — 10

pwc

Syntax	pwc [previous]
Context	<GLOBAL>
Description	This command displays the present or previous working context of the CLI session. The pwc command provides a user who is in the process of dynamically configuring a chassis a way to display the current or previous working context of the CLI session. The pwc command displays a list of the CLI nodes that hierarchically define the current context of the CLI instance of the user. For example: <pre>A:Dut-G>config>service>vpls# pwc ----- Present Working Context : ----- <root> configure service vpls 1 ----- A:Dut-G>config>service>vpls#</pre> 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.
Parameters	previous — Specifies to display 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.
Parameters	<i>seconds</i> — The number of seconds for the console session to sleep, expressed as a decimal integer.
	Default 1
	Values 1 — 100

ssh

Syntax	ssh [<i>ip-addr</i> <i>dns-name</i> <i>username@ip-addr</i>] [-l <i>username</i>] [-v <i>SSH-version</i>] [router <i>router-instance</i>]
Context	<GLOBAL>
Description	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. 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.
Parameters	<i>ip-address</i> <i>host-name</i> — The remote host to which to open an SSH session. The IP address or the DNS name (providing DNS name resolution is configured) can be specified. -l <i>user</i> — The user name to use when opening the SSH session. router <i>router-instance</i> — Specify the router name or service ID. Values <i>router-name:</i> Base, management (supported only on 7210 SAS-E), vpls-management. Default Base

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 7210 SAS networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries. The number of retry attempts for a Telnet client session is not user-configurable.

Parameters	<i>ip-address</i> — The IP address or the DNS name (providing DNS name resolution is configured) can be specified.		
	Values	ipv4-address	a.b.c.d
		ipv6-address	x::x::x::x::x::x (eight 16-bit pieces) x::x::x::x::x::d.d.d.d x: [0 .. FFFF]H d: [0 .. 255]D
	dns-name — Specify the DNS name (if DNS name resolution is configured).		
	Values	128 characters maximum	
	<i>port</i> — The TCP port number to use to Telnet to the remote host, expressed as a decimal integer.		
	Default	23	
	Values	1 — 65535	
	router <i>router-instance</i> — Specify the router name or service ID.		
	Values	<i>router-name:</i>	Base, management (supported only on 7210 SAS-E) ,vpls-man- agement.
	Default	Base	

traceroute

Syntax	traceroute [<i>ip-address</i> <i>dns-name</i>] [ttl <i>tvl</i>] [wait <i>milliseconds</i>] [no-dns] [source <i>ip-address</i>] [tos <i>type-of-service</i>] [router <i>router-instance</i>]		
Context	<GLOBAL>		
Description	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. 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#		
Parameters	<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.		
	Values	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.d x: [0 .. FFFF]H d: [0 .. 255]D
	tvl <i>tvl</i> — The maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer.		
	Values	1 — 255	

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

Default 5000

Values 1 — 60000

no-dns — When the **no-dns** keyword is specified, 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 — 255

router *router-instance* — Specifies the router name or service ID.

Values *router-name:* Base, management (supported only on 7210 SAS-E), vpls-management.
service-id: 1 — 2147483647

Default Base

tree

Syntax	tree [detail]
Context	<GLOBAL>
Description	This command displays the command hierarchy structure from the present working context.
Parameters	detail — Includes parameter information for each command displayed in the tree output.

write

Syntax	write { <i>user</i> broadcast } <i>message-string</i>
Context	<GLOBAL>
Description	This command sends a console message to a specific user or to all users with active console sessions.
Parameters	<i>user</i> — The name of a user with an active console session to which to send a console message. Values Any valid CLI username broadcast — Specifies that the <i>message-string</i> is to be sent to all users logged into the router. <i>message-string</i> — 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.

CLI Environment Commands

alias

Syntax	alias <i>alias-name</i> <i>alias-command-line</i> no alias <i>alias-name</i>
Context	environment
Description	This command enables the substitution 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. Only a single command can be present in the command string. The alias command can be entered in any context but must be created in the root>environment context. For example, to create an alias named soi to display OSPF interfaces, enter: alias soi "show router ospf interface"
Parameters	<i>alias-name</i> — The alias name. Do not use a valid command string for the alias. If the alias specified is an actual command, this causes the command to be replaced by the alias. <i>alias-command-line</i> — 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 [<i>number of nodes in prompt</i>] no reduced-prompt
Context	environment
Description	This command configures the maximum number of higher CLI context levels to display in the CLI prompt for the current CLI session. This command is useful when configuring features that are several node levels deep, causing the CLI prompt to become too long. By default, the CLI prompt displays the system name and the complete context in the CLI. The number of <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 (“...”). <pre>A:ALA-1>environment# reduced-prompt 2 A:ALA-1>vonfig>router# interface to-103 A:ALA-1>...router>if#</pre> Note that the setting is not saved in the configuration. It must be reset for each CLI session or stored in an exec script file. The no form of the command reverts to the default.
Default	no reduced-prompt — Displays all context nodes in the CLI prompt.
Parameters	<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. Default 2 Values 0 — 15

saved-ind-prompt

Syntax	[no] saved-ind-prompt
Context	environment
Description	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. <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>

terminal

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

length

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

time-display

Syntax	time-display { local utc }
Context	environment
Description	This command displays time stamps in the CLI session based on local time or Coordinated Universal Time (UTC). The system keeps time internally in UTC and is capable of displaying the time in either UTC or local time based on the time zone configured. This configuration command is only valid for times displayed in the current CLI session. This includes displays of event logs, traps and all other places where a time stamp is displayed. 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.
Default	time-display local — Displays time stamps based on the local time.

time-stamp

Syntax	time-stamp
Context	environment
Description	This command displays time stamps in the CLI session.

Monitor CLI Commands

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> [<i>interval seconds</i>] [<i>repeat repeat</i>] [<i>absolute</i> <i>rate</i>]
Context	monitor>filter
Description	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. 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. 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	<i>ip-filter-id</i> — Displays detailed information for the specified filter ID and its filter entries. Values 1 — 65535 <i>entry entry-id</i> — Displays information on the specified filter entry ID for the specified filter ID only. Values 1 — 65535 <i>interval seconds</i> — Configures the interval for each display in seconds. Default 5 seconds Values 3 — 60 <i>repeat repeat</i> — Configures how many times the command is repeated. Default 10 Values 1 — 999 absolute — When the absolute keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics. rate — When the rate keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

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	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.

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.

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 — 65535

entry *entry-id* — Displays information on the specified IPv6 filter entry ID for the specified filter ID only.

Values 1 — 65535

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

Default 10 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

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

Sample Output

```
*A:7210SAS>monitor>filter# ipv6 10 entry 10 interval 3 repeat 3 absolute
```

```
=====
Monitor statistics for IPv6 filter 10 entry 10
=====
```

```
-----
At time t = 0 sec (Base Statistics)
-----
```

```
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts
```

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

```
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts
```

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

```
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts
```

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

```
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts
```

```
=====
*A:7210SAS>monitor>filter#
```

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

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 lag-id [lag-id...(up to 5 max)] [interval seconds] [repeat repeat] [absolute rate]
Context	monitor
Description	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. 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. 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 *lag-id* — The number of the LAG.

Default none — The LAG ID value must be specified.

Values 1 — 6

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

Default 5 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

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

Sample Output

```
A:ALA-12# monitor lag 2
=====
Monitor statistics for LAG ID 2
=====
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.

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 nonitors statistics for the MAF IP filter entry.
Parameters	entry <i>entry-id</i> — Specifies an existing IP MAF entry ID. Values 1 — 9999 <i>interval seconds</i> — Configures the interval for each display in seconds. Default 10 Values 3 — 60 repeat <i>repeat</i> — Configures how many times the command is repeated. Default 10 Values 1 — 999 absolute — When the absolute keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics. rate — When the rate keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

ipv6

Syntax	ipv6 entry-id [<i>interval seconds</i>] [<i>repeat repeat</i>] [<i>absolute</i> <i>rate</i>]
Context	monitor>management-access-filter
Description	This command nonitors statistics for the MAF IPv6 filter entry.
Parameters	entry <i>entry-id</i> — Specifies an existing IP MAF entry ID. Values 1 — 9999 <i>interval seconds</i> — Configures the interval for each display in seconds. Default 10 Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

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

port

Syntax **port** *port-id* [*port-id...*(up to 5 max)] [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command enables port traffic monitoring. The specified port(s) statistical information displays at the configured interval until the configured count is reached.

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. 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 **port** *port-id* — Specify up to 5 port IDs.

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

Default 5 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

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

Sample Output

```
A:ALA-12>monitor# port 1/1/4 interval 3 repeat 3 absolute
```

```
=====
Monitor statistics for Port 1/1/4
=====
```

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 1/1/4 interval 3 repeat 3 rate
=====
Monitor statistics for Port 1/1/4
=====
                                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
-----
At time t = 6 sec (Mode: Rate)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0
-----
At time t = 9 sec (Mode: Rate)
-----
Octets                                0                                0
Packets                              0                                0
Errors                                0                                0
=====
A:ALA-12>monitor#
```

service

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

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 <i>service-id</i>. 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.
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> [<i>interval seconds</i>] [<i>repeat repeat</i>] [<i>absolute</i> <i>rate</i>]								
Context	monitor>service>id <i>service-id</i>								
Description	This command monitors statistics for a SAP associated with this service. This command displays statistics for a specific SAP, identified by the <i>port-id</i> 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.								
Parameters	<i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition. Values <i>sap-id</i>: <table> <tr> <td>null</td><td>[<i>port-id</i> <i>lag-id</i>]</td></tr> <tr> <td>dot1q</td><td>[<i>port-id</i> <i>lag-id</i>]:* <i>qtag</i></td></tr> <tr> <td>qinq</td><td>[<i>port-id</i> <i>lag-id</i>]:qtag1.qtag2</td></tr> <tr> <td>port-id</td><td><i>slot/mda/port</i></td></tr> </table>	null	[<i>port-id</i> <i>lag-id</i>]	dot1q	[<i>port-id</i> <i>lag-id</i>]:* <i>qtag</i>	qinq	[<i>port-id</i> <i>lag-id</i>]:qtag1.qtag2	port-id	<i>slot/mda/port</i>
null	[<i>port-id</i> <i>lag-id</i>]								
dot1q	[<i>port-id</i> <i>lag-id</i>]:* <i>qtag</i>								
qinq	[<i>port-id</i> <i>lag-id</i>]:qtag1.qtag2								
port-id	<i>slot/mda/port</i>								

```

lag-id lag-id
      lag keyword
      id 1 — 200
qtag1 0 — 4094
qtag2 *, 0 — 4094

```

port-id — Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the *slot_number/MDA_number/port_number* format. For example 1/2/3 specifies port 3 on MDA 2 in slot 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 — 4094
 qtag2 : * | 0 — 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.

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	0	The SAP is identified by the port.
Ethernet	Dot1q	0 — 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 — 4094 qtag2: 0 — 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.

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

Default 11 seconds

Values 11 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the absolute rate-per-second value for each statistic is displayed.

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

Sample Output

```

A:7210SAS-E>monitor>service>id# sap 1/1/1:100
=====
Monitor statistics for Service 10000 SAP 1/1/1:100

```

```

=====
-----
At time t = 110 sec (Mode: Delta)
-----
-----
Ingress QoS Classifier Usage
-----
Classifiers Allocated: 16 Meters Allocated : 8
Classifiers Used : 2 Meters Used : 2
-----
Sap Statistics
-----
Packets Octets
Ingress Stats: 1013264 0
Egress Stats: 163674 0
-----
Sap STP Statistics
-----
Forward transitions : 0 Bad BPDUs rcvd : 0
Cfg BPDUs rcvd : 0 Cfg BPDUs tx : 0
TCN BPDUs rcvd : 0 TCN BPDUs tx : 0
RST BPDUs rcvd : 0 RST BPDUs tx : 0
MST BPDUs rcvd : 0 MST BPDUs tx : 0
-----
Sap per Meter Stats
-----
Packets Octets
Ingress Meter 1 (Unicast)
For. InProf : 0 0
For. OutProf : 210645 0
Ingress Meter 11 (Multipoint)
For. InProf : 0 0
For. OutProf : 87238 0
=====
A:7210SAS-E>monitor>service>id#

```

Show Commands

alias

Syntax	alias
Context	<root>
Description	This command displays a list of existing aliases.
Output	Show Alias Fields — The following table describes alias output fields.

Table 11: 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
ssi                        show service service-using ies
-----
Number of aliases : 5
=====
A:ALA-103>config>system#
```


File System Management

In This Chapter

This chapter provides information about file system management.

Topics in this chapter include:

- [The File System on page 82](#)
 - [Compact Flash Devices on page 82](#)
 - [USB Storage Device on page 83](#)
 - [URLs on page 79](#)
 - [Wildcards on page 86](#)
- [File Management Tasks on page 87](#)
 - [Modifying File Attributes on page 81](#)
 - [Creating Directories on page 88](#)
 - [Copying Files on page 89](#)
 - [Moving Files on page 90](#)
 - [Removing Files and Deleting Directories on page 90](#)
 - [Displaying Directory and File Information on page 91](#)

The File System

The 7210 SAS 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.

Compact Flash Devices

The file system is based on a DOS file system.

In 7210 SAS, the node has a single compact flash (internal). The name of this compact flash device is "cfl:",

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 compact flash devices on the 7210 SAS devices are non-removable.

Note: From release 4.0R2 , a warning message is displayed on the console and a trap (tmnxRootDirFull) is generated if the number of files and directories in the root directory crosses the threshold limit of "80". A warning will be generated for every new file or directory created after threshold limit is exceeded. This limit is applicable only for files and directories created in the root directory on cfl:\. There is no restriction on the number of files and directories created in the sub-directories. The number of files in the root directory might also increment by issuing the command "admin save" or "bof save". When this event is displayed it is expected that the user cleans up the root directory and removes the unnecessary files and directories or moves them to a sub-directory created under the root-directory to ensure that the number of entries (files or directories) in the root directory is below the limit. No warning is generated when the number of files and directories comes down below the threshold.

The number of files or directories present in the root directory can be determined by using the command "file dir cfl:\". For example:

```
*A:7210-SAS #  
  
*A:7210-SAS #file dir  
  
Volume in drive cfl on slot A is /flash.  
  
Volume in drive cfl on slot A is formatted as FAT32.  
  
Directory of cfl:\
```

```

10/12/2011  10:37p                4248394 boot.tim
10/17/2011  07:28a                 524 sasm.sdx
10/26/2011  10:06p                 828 bof.cfg
10/27/2011  09:04p      <DIR>      act-collect
10/27/2011  09:06p      <DIR>      act
10/17/2011  07:30a                 0 test1.txt
10/26/2011  10:43p                5360 sasm.cfg
10/11/2011  06:42a            28821599 both.tim
10/26/2011  10:42p            14597 bootlog.txt
10/19/2011  04:22a                 832 bof.cfg.1
10/17/2011  07:37a                 827 test1
10/17/2011  07:38a                 827 tes2
10/17/2011  07:38a                 827 tes3
10/17/2011  07:39a                 827 tes3567
10/17/2011  07:38a                 827 tes356
10/18/2011  10:46p            5481 sasm.cfg.1

          14 File(s)                33117369 bytes.
           2 Dir(s)                80470016 bytes free.

*A:7210-SAS #

```

In the above example, the total of files and directories is 14 files + 2 directories = 16.

USB Storage Device

Note : USB devices are supported only on 7210 SAS-E devices.

7210 SAS-7210 SASE platform supports USB interface which provides storage functionality. It supports USB version 1.1. It allows the use of USB sticks providing them an alternate storage location with larger capacity than the internal flash. The USB storage device is identified as ufl: by the system and supports DOS file system.

The USB storage device can be used to store Timos images, configuration files, accounting records, and log files. The BOF file can point to images on USB and be used to load Timos images and configuration files.

NOTE:

- During bootup, the system USB storage cannot be used to load boot.tim (that is, the bootloader). Hence, the bootloader required to boot the device must be stored on the compact flash (cfl).
- The list of USB devices and capacities that is supported for use with 7210 SAS are:
 - Cruzer Fit – size 4GB and 8GB
 - Cruzer Blade – size 4GB and 8GB

Note: USB models from Sandisk are supported.

- When an USB device is unplugged or removed from the system a major alarm is raised. The alarm can be cleared using the shutdown command.
- 7210 SAS also autodetects the device type when any of the supported devices are connected to the USB interface. Only approved USB mass storage device and optical clip-on devices can be plugged in to the USB port and are recognized as valid devices. All other unsupported devices will result in an error log being printed.
- It is highly recommended to use the “shutdown” command before removing the USB storage device.

URLs

The arguments for the 7210 SAS 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*).

7210 SAS 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 12](#).

Table 12: URL types and Syntax

URL Type	Syntax	Notes
<i>local-url</i>	<i>[cflash-id:\]path</i> <i>[usb-flash-id:\]path</i>	<i>cflash-id</i> is the compact flash device name. Values: cfl: <i>usb-flash-id</i> is the USB device name. Values: ufl:
<i>ftp-url</i>	ftp:// <i>[username[:password]@]host/path</i> ftp:// <i>[username[:password]@]host/./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 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[/path]/filename</i>	tftp is only supported for operations on file-urls.

The system accepts either forward slash (“/”) or backslash (“\”) characters to delimit directory and/or filenames in URLs. Similarly, the 7210 SAS 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.

Wildcards

7210 SAS OS 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 cfl:\ # copy test*.cfg siliconvalley
 cfl:\testfile.cfg
 1 file(s) copied.
 A:ALA-1>file cfl:\ # cd siliconvalley
 A:ALA-1>file cfl:\siliconvalley\ # dir
 Volume in drive cfl on slot A has no label.
 Directory of cfl:\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 cfl:\siliconvalley\ #

All the commands can operate on the local file system. [Table 13](#) indicates which commands also support remote file operations.

Table 13: 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	
md		X	
move	X	X	
rd		X	
scp	source only		
type	X	X	X
version	X	X	X

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 on page 81](#)
 - [Creating Directories on page 88](#)
 - [Copying Files on page 89](#)
 - [Moving Files on page 90](#)
 - [Removing Files and Deleting Directories on page 90](#)
 - [Displaying Directory and File Information on page 91](#)
-

The following displays the file configuration:

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

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 displays an example of the command syntax:

Example: `file cf1:\ # md test1`
`file 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 #`

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.cfg cf1:\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 cf1:/file3 admin@192.168.x.x:cf1:\file3`

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\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\ #
  
```

Removing Files and Deleting Directories

Use the `delete` and `rd` commands to delete files and remove directories. Directories must be empty in order to delete them. When file or directories are deleted they cannot be recovered.

Use the CLI syntax displayed below to delete files and 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:\ #
  
```

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 cpm.tim or iom.tim file.

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

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

The following displays an example of the command syntax:

```
*A:card-1>file cfl:\ # dir
  Volume in drive cfl on slot A is /flash.

  Volume in drive cfl on slot A is formatted as FAT32.

Directory of cfl:\

10/22/2008  10:30a                8849 bootlog.txt
10/22/2008  10:30a                 733 bof.cfg
10/22/2008  10:29a                5531 bootlog_prev.txt
02/01/2001  09:25a            3528373 boot.tim
02/01/2001  09:21a                4860 config.cfg
10/22/2008  11:07a      <DIR>          test1
10/17/2008  07:32p                 724 env.cfg
10/15/2008  03:38p            9499 snake.cfg
              7 File(s)              3558569 bytes.
              1 Dir(s)              53135360 bytes free.
```

File Command Reference

Command Hierarchy

Configuration Commands

file

- **attrib** [+r | -r] *file-url*
- **attrib**
- **cd** [*file-url*]
- **copy** *source-file-url dest-file-url* [**force**]
- **delete** *file-url* [**force**]
- **dir** [*file-url*] [sort-order {d | n | s}] [reverse]
- **md** *file-url*
- **move** *old-file-url new-file-url* [**force**]
- **rd** *file-url* rf [**force**]
- **scp** *local-file-url destination-file-url* [**router router-instance**] [**force**]
- [**no**] **shutdown** *cflash-id*
- **type** *file-url*
- **version** *file-url* [**check**]

Configuration Commands

File System Commands

shutdown

Syntax	[no] shutdown [cflash-id]
Context	file
Description	This command is available for use only with USB storage drives or sticks and cannot be used with the internal compact flash cf1:\. Use the no shutdown [cflash-id] command to enable a USB drive (uf1:\) for use as a storage device on the node. NOTE: Do not remove the USB drive during a read/write operation.
Default	no shutdown — compact flash device administratively enabled.
Parameters	<i>cflash-id</i> — Enter the USB ID (only uf1:\ is allowed) to be shut down or enabled. When a specific cflash-id is specified, then that drive is shutdown.
Default	None
Values	uf1:\

File Commands

attrib

Syntax	attrib [+r -r] <i>file-url</i> attrib
Context	file
Description	This command sets or clears/resets the read-only attribute for a file in the local file system. To list all files and their current attributes enter attrib or attrib x where x is either the filename or a wildcard (*). When an attrib command is entered to list a specific file or all files in a directory, the file's attributes are displayed with or without an "R" preceding the filename. The "R" implies that the +r is set and that the file is read-only. Files without the "R" designation implies that the -r is set and that the file is read-write-all. For example: <pre> ALA-1>file cfl:\ # attrib cfl:\bootlog.txt cfl:\bof.cfg cfl:\boot.ldr cfl:\srl.cfg cfl:\test cfl:\bootlog_prev.txt R cfl:\BOF.SAV </pre>
Parameters	<i>file-url</i> — The URL for the local file.
Values	<local-url> <remote-url> - [255 chars max] local-url - [<cflash-id>/ <usb-flash-id>/][<file-path>] remote-url - [{ftp:// tftp://} <login>:<pswd>@<remote-locn>/][<file-path>] remote-locn - [<hostname> <ipv4-address> "["<ipv6-address>"]"] ipv4-address - a.b.c.d ipv6-address - x:x:x:x:x:x:x:x[-interface] x - [0..FFFF]H d - [0..255]D interface - 32 chars max, for link local addresses cflash-id - cfl: usb-flash-id - ufl: Note: USB flash is supported only on 7210 SAS-E. +r — Sets the read-only attribute on the specified file. -r — Clears/resets the read-only attribute on the specified file.

cd

Syntax	cd [<i>file-url</i>]
Context	file
Description	This command displays or changes the current working directory in the local file system.
Parameters	<i>file-url</i> — Syntax: [<local-url> <remote-url> - [255 chars max] local-url - [<cflash-id>/ <usb-flash-id>/][<file-path>] remote-url - [{ftp:// tftp://}<login>:<pswd>@<remote-locn>/][<file-path>] 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: usb-flash-id - uf1: Note: USB flash is supported only on 7210 SAS-E. <none> — Displays the current working directory. .. — Signifies the parent directory. This can be used in place of an actual directory name in a <i>directory-url</i>. <i>directory-url</i> — The destination directory.

copy

Syntax	copy <i>source-file-url dest-file-url</i> [force]
Context	file
Description	This command copies a file or all files in a directory from a source URL to a destination URL. At least one of the specified URLs should be a local URL. The optional wildcard (*) can be used to copy multiple files that share a common (partial) prefix and/or (partial) suffix. When a file is copied to a destination with the same 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: “Overwrite destination file (y/n)?” For example: To copy a file named srcfile in a directory called <i>test</i> on <i>cf1</i> to a file called destfile in a directory called <i>production</i> on <i>cf1</i>, the syntax is: <pre>src1>file cf1:\ # copy cf2-/test/srcfile/production/destfile</pre>

File Commands

To FTP a file named **121201.cfg** in directory *mydir* stored on *cf1* 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:

```
copy /mydir/121201.cfg 131.12.31.79/backup/121201.cfg
```

Parameters *source-file-url* — The location of the source file or directory to be copied.

dest-file-url — The destination of the copied file or directory.

Values	<file-url>	: <local-url> <remote-url> - [255 chars max]
	local-url	- [<cf1ash-id>/ <usb-flash-id>/][<file-path>]
	remote-url	- [{ftp:// tftp://}<login>:<pswd>@<remote-locn>/][<file-path>]
	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
	cf1ash-id	- cf1:
	usb-flash-id	- uf1:

Note: USB flash is supported only on 7210 SAS-E.

force — Forces an immediate copy of the specified file(s).

Values	<file-url>	: <local-url> <remote-url> - [255 chars max]
	local-url	- [<cf1ash-id>/][<file-path>]
	remote-url	- [{ftp:// tftp://}<login>:<pswd>@<remote-locn>/][<file-path>]
	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
	cf1ash-id	- cf1:
	usb-flash-id	- uf1:

Note: USB flash is supported only on 7210 SAS-E.

file copy force executes the command without displaying a user prompt message.

delete

Syntax	delete <i>file-url</i> [force]
Context	file
Description	This command deletes the specified file. The optional wildcard “*” can be used to delete multiple files that share a common (partial) prefix and/or (partial) suffix. When the wildcard is entered, the following prompt displays for each file that matches the wildcard: “Delete file <filename> (y/n)?” <i>file-url</i> — The file name to delete. Values <local-url> <remote-url> - [255 chars max] local-url - [<cflash-id>/ <usb-flash-id>][<file-path>] remote-url - [ftp://<login>:<pswd>@<remote-locn>/] [<file-path>] remote-locn - [<hostname> <ipv4-address> "["<ipv6-address>"]"] ipv4-address - a.b.c.d ipv6-address - x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:d.d.d.d[-interface] x - [0..FFFF]H d - [0..255]D interface - 32 chars max, for link local addresses cflash-id - cfl: usb-flash-id - ufl: Note: USB flash is supported only on 7210 SAS-E. force — Forces an immediate deletion of the specified file(s). file delete * force deletes all the wildcard matching files without displaying a user prompt message.

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.
Parameters	<i>file-url</i> — The path or directory name. Values <local-url> <remote-url> - [255 chars max] local-url - [<cflash-id>/ <usb-flash-id>][<file-path>] remote-url - [ftp://<login>:<pswd>@<remote-locn>/]

File Commands

```
[<file-path>]
remote-locn  - [ <hostname> | <ipv4-address> |
               "["<ipv6-address>"]" ]
ipv4-address  - a.b.c.d
ipv6-address  - x:x:x:x:x:x:x:x[-interface]
               x:x:x:x:x:x:d.d.d.d[-interface]
               x - [0..FFFF]H
               d - [0..255]D
               interface - 32 chars max, for link
                           local addresses
cflash-id    - cfl:
usb-flash-id - ufl:
```

Note: USB flash is supported only on 7210 SAS-E.

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

sort-order { d | n | s } — Specifies the sort order.

Values

- d — date
- n — name
- s — size

reverse — Specifies to reverse the sort order.

Default Lists all files in the present working directory

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.

md

Syntax	md <i>file-url</i>
Context	file
Description	This command creates a new directory in a file system.

Directories can only be created one level at a time.

Parameters *file-url* — The directory name to be created.

Values <local-url>|<remote-url> - [255 chars max]
 local-url - [<cf-flash-id>/|<usb-flash-id>/][<file-path>]
 remote-url - [ftp://<login>:<pswd>@<remote-locn>/]
 [<file-path>]
 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
 cf-flash-id - cf1:
 usb-flash-id - ufl:

Note: USB flash is supported only on 7210 SAS-E.

move

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

Context file

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

The following prompt appears if the destination file already exists:

“Overwrite destination file (y/n)?”

Parameters *old-file-url* — The file or directory to be moved.

Values <local-url>|<remote-url> - [255 chars max]
 local-url - [<cf-flash-id>/|<usb-flash-id>/][<file-path>]
 remote-url - [ftp://<login>:<pswd>@<remote-locn>/]
 [<file-path>]
 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
 cf-flash-id - cf1:

File Commands

usb-flash-id - ufl:

Note: USB flash is supported only on 7210 SAS-E.

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

Values <local-url>|<remote-url> - [255 chars max]
 local-url - [<cflash-id>/|<usb-flash-id>/][<file-path>]
 remote-url - [ftp://<login>:<pswd>@<remote-locn>/]
 [<file-path>]
 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 - cfl:
 usb-flash-id - ufl:

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

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

rd

Syntax	rd <i>file-url</i> rf [force]
Context	file
Description	The rd command is used to delete a directory. If a directory has files and no sub-directories, the force option must be used to force delete the directory and files it contains.
Parameters	<i>file-url</i> — The directory to be removed. Values local-url remote-url - [255 chars max] local-url [<cflash-id>/ <usb-flash-id>/][<file-path>] remote-url [ftp://login:pswd@remote-locn/][file-path] 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 cfl:

usb-flash-id - ufl:

Note: USB flash is supported only on 7210 SAS-E.

rf — The parameter forces a recursive delete.

force — Forces an immediate deletion of the specified directory.

For example, **rd file-url force** executes the command without displaying a user prompt message.

repair

Syntax	repair [<i>cflash-id</i>]
Context	file
Description	This command checks a compact flash device for errors and repairs any errors found.
Parameters	<i>cflash-id</i> — Specify the compact flash slot ID to be shut down or enabled. When a specific cflash-id is specified, then that drive is shutdown. If no cflash-id is specified, the drive referred to by the current working directory is assumed. Default The current compact flash device. Values cfl:, ufl:

scp

Syntax	scp <i>local-file-url</i> <i>destination-file-url</i> [router <i>router-instance</i>] [force]
Context	file
Description	This command copies a local file to a remote host file system. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH. The following prompt appears: “Are you sure (y/n)?” The destination must specify a user and a host.
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 user@hostname:destination-file <i>user</i> — The SSH user. <i>host</i> — The remote host IP address or DNS name. <i>file-path</i> — The destination path. <i>router-instance</i> — Specify the router name or service ID. Values <i>router-name</i>: Base , management <i>service-id</i>: 1 — 2147483647

Default Base

force — Forces an immediate copy of the specified file.

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

type

Syntax	type <i>file-url</i>
Context	file
Description	Displays the contents of a text file.

version

Syntax	version <i>file-url</i> [check]
Context	file
Description	This command displays the version of a TiMOS file.
Parameters	<i>file-url</i> — The file name of the target file.

Values	<local-url> <remote-url> - [255 chars max]
	local-url - [<cflash-id>/ <usb-flash-id>/][<file-path>]
	remote-url - [ftp://<login>:<pswd>@<remote-locn>/] [<file-path>]
	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 - cfl:
	usb-flash-id - ufl:

Note: USB flash is supported only on 7210 SAS-E.

check — Validates the *.tim* file.

vi

Syntax	vi <i>local-url</i>
Context	file
Description	Edit files using the vi editor.
Parameters	<i>local-url</i> — Specifies the local source file or directory.
Values	[cflash-id>/]file-path <i>cflash-id</i> : <i>cfl</i> :, <i>ufl</i> :

Boot Options

In This Chapter

This chapter provides information about configuring boot option parameters.

Topics in this chapter include:

- [System Initialization on page 108](#)
 - [Manual Mode on page 111](#)
 - [Auto Init on page 112](#)
 - [Ping Check on page 118](#)
 - [Persistence on page 119](#)
- [Initial System Startup Process Flow on page 126](#)
- [Configuration Notes on page 127](#)

System Initialization

When the system is powered ON it executes the bootstrap image, for example, the boot.tim file, from the file system which is located on a non-removable flash device (cfl:) that is built in to the 7210 SAS-Series router. The boot.tim file is the image that reads and executes the system initialization commands configured in the Boot Option File (BOF). The default behavior is to initially search for the boot.tim file on cfl:. This behavior cannot be modified. If the boot.tim file is not present, or is not a valid loadable file, the Golden bootstrap image is loaded by the bootrom. This image is equivalent to a boot.tim file except that it is present outside the file system and can be updated and checked by means of special CLI commands.

When the system executes boot.tim, provision is given to the user to modify the BOF manually and save it or to boot using existing BOF. The bootstrap image then processes the BOF file present in the flash as explained in [Configuration and Image Loading on page 114](#). The system is shipped to the customer site with a boot.tim file and a Golden bootstrap image, but without a BOF file. When the system is powered ON for the first time, there will be no BOF in the system. Hence, provisions are given to create a new BOF file or alternatively get the BOF file from the network. There are two options:

- Boot by manually creating a BOF file (manual boot).
- Boot by retrieving the BOF file from the network, using DHCP to get the network location of the BOF file (auto init). Auto-init is the default boot procedure if there is no manual-intervention during the first-time boot of the node.

Note: When the operator executes the **reset** command in the boot loader prompt or **admin reboot auto-init** in the TiMos CLI, 7210 SAS resets the current BOF and reboots.

Note: The operator can manage a 7210 SAS E node through an external physical network. Managing a node through an external physical network secures the management network by restricting access to service customers and service data. The 7210 SAS E node can be managed through the Out-of-band (OOB) Ethernet management port. The 7210 SAS-D devices do not support Out-of-band Ethernet management port.

The following is an example of console display output when the boot.tim file is located on *cfl* and the system boots successfully.

```
Alcatel-Lucent 7210 Boot ROM. Copyright 2000-2009 Alcatel-Lucent.  
All rights reserved. All use is subject to applicable license agreements.  
Running POST tests from ROM  
Testing ROM load area...done  
  
Relocating code...Jumping to RAM  
  
Performing second stage RAM test....passed  
  
Board Serial Number is 'SN123456789'  
Bootlog started for Version V-0.0.I317  
Build V-0.0.I317 bootrom/mpc 7xxx
```

```
Built on Tue Jan 6 02:23:14 IST 2009 by panosbld in /panosbld/ws/panos/main

?Attempting to load from file cfl:/boot.tim
Version L-0.0.I312, Fri Jan 2 04:26:32 IST 2009 by panosbld in /panosbld/ws/panos/main
text:(3002475-->12623392) + data:(550940-->2414128)
Starting at 0xb000000...

Total Memory: 512MB Chassis Type: sas Card Type: badami_7210
TiMOS-L-0.0.I312 boot/mpc ALCATEL SAS-E 7210 Copyright (c) 2000-2009 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Fri Jan 2 04:26:32 IST 2009 by panosbld in /panosbld/ws/panos/main

TiMOS BOOT LOADER

...
```

Figure 3 displays the bootstrap load process.

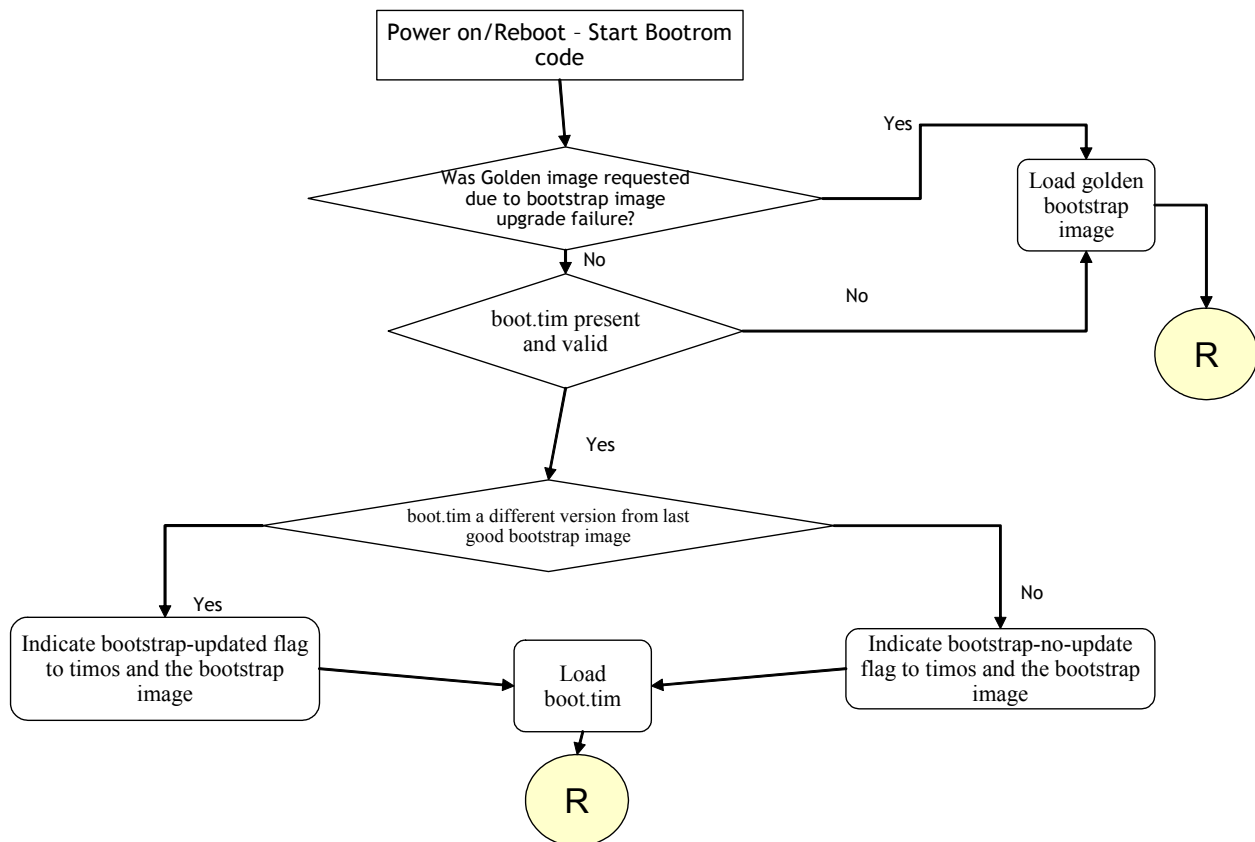


Figure 3: Bootstrap Load Process - System Initialisation - Part I

Figure 4 displays the flash directory structure and file names.

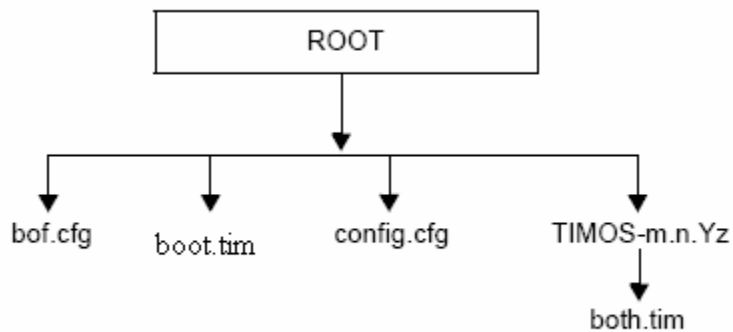


Figure 4: Files on the Flash

Files on the compact flash are:

- bof.cfg — Boot option file
- boot.tim — 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

Manual Mode

Note: Out-of-Band Ethernet management port is not supported on 7210 SAS-D devices.

If the user opts for the manual-mode boot procedure for the first time boot, the required parameters must be specified for a successful system boot. Manual mode configurations require authentication. The default password is **password**. BOF parameters that should be configured include:

- Image path
- Configuration file path
- UplinkA parameters (port number, vlan ID, IP/mask, static route)
- UplinkB parameters (port number, vlan ID, IP/mask, static route)
- eth-mgmt-disable (supported only on 7210 SAS-E)

Provisions to configure two uplinks is given in the BOF for port redundancy. If the image path and configuration file path are local, then the IP address and routing information for uplinkA and uplinkB are not required. The user can optionally obtain IP parameters through DHCP by configuring 0 (zero) for the uplink port's IP address. In this case, the DHCP server should be configured to grant the IP address and the default gateway information used to reach the server where the image and configuration files are present. After the BOF configuration is completed, a BOF with configured parameters is created in the flash that can be used for subsequent reboots. The bootstrap image then processes the BOF parameters in order to boot the system. BOF processing is explained in [Configuration and Image Loading on page 114](#).

For 7210 SAS-E devices, **eth-mgmt-disable** parameter indicates if the out-of-band Ethernet management port is enabled during the boot-up procedure. The 7210 SAS-D devices do not support Out-of-band Ethernet management port. For a 7210 node which has a previous BOF, the boot process uses the existing parameters for uplink A and uplink B ports to boot the TIMOS image. The OOB port is disabled, by default.

Auto Init

During the first boot or a reboot after the execution of CLI command **admin reboot auto-init**, if the user does not intervene to create the BOF file in the manual mode, the system, by default, goes to auto-init procedure after a “wait” time. The default wait time is 3 seconds. There are two designated ports used for auto init. These are the front panel ports, port 1 and port 2. Auto init requires a DHCP server to be configured in the network which should be reachable by the system. DHCP requests are directed out of one uplink port at a time. All other ports of the system would be down.

If a DHCP server is present in the network, the system expects to receive an IP address, the default gateway information, and BOF file path in the response returned by the DHCP server. Upon receiving these parameters from DHCP server, the system will apply the IP configuration and then download the BOF file from the path given by the DHCP server. The BOF file is then saved into the flash and is used for subsequent reboots. The bootstrap image then processes the BOF parameters in order to boot the system. BOF processing is explained in [Configuration and Image Loading on page 114](#)

The system first attempts to use uplinkA and then uplinkB parameters to receive a successful response from the DHCP server. If there is no response from the DHCP server on both the uplink ports, the boot procedure is restarted, during which the user can opt to enter the manual mode or allow the system to default to auto-init again.

Configuration Guidelines for use of Auto-init and Manual mode

- Ethernet management port does not support AutoInit mode. The use of DHCP to obtain the BOF file from the network and other system parameters is currently not supported on Ethernet management port.
- In autoinit mode, DHCP requests sent out by the node are in two formats. The system attempts to communicate with the DHCP server in these two formats, one after another(if necessary).
 - Initially, the DHCP requests are sent out with a priority VLAN tag (VLAN ID = 0, Dot1p PCP bits set to 7).
 - If no response is received from the DHCP server during the above request period, DHCP requests are sent without VLAN tags (that is, null-tagged packets).
- In autoinit mode, DHCP client expects the following options to contain the BOF file name and the server IP address. BOF file can be downloaded through FTP or TFTP based on the

information a client receives from DHCP server. Listed below are the ways in which DHCP client will try to obtain the file:

- **1. Using the vendor specific option** : The client searches for the option “43” in the DHCP reply. This provides the URL which has to be accessed through FTP. For example: *ftp://abcd:xyz@10.0.0.2/test/bof.cfg*. If this file is found the client retrieves this file.
- **2. Collating server-name and file-name** : If the option “43” is not found in the DHCP reply, then a URL has to be formed by using the tftp-server name and the boot-file retrieved via TFTP. IP address of TFTP server is obtained from DHCP Option “66” or the "sname" field of a DHCP message and filename on the TFTP server is obtained from DHCP Option “67” or the "file" field of a DHCP message.
- In the manual mode, if the OOB port is enabled (that is the “eth-mgmtdisable” is set to “no”), the OOB port is used to download the TIMOS image file and configuration file specified in the BOF file, and the system boot is successfully completed. If a system boot fails, the uplink A and uplink B parameters are used to retrieve the TIMOS image and configuration files.

Configuration and Image Loading

The bootstrap image processes the initialization parameters from the BOF. The bootstrap image attempts to locate the configuration file as configured in the BOF. Up to 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. If the configuration file is in a remote location, the bootstrap process saves it on the flash as `cf1:/default.cfg`. Users must not delete this file or create a file with this name. The configuration file includes chassis, MDA, and port configurations, as well as system, routing, and service configurations. Like the configuration file, 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. [Figure 5](#), [Figure 6](#), and [Figure 7](#) describe the bootstrap process.

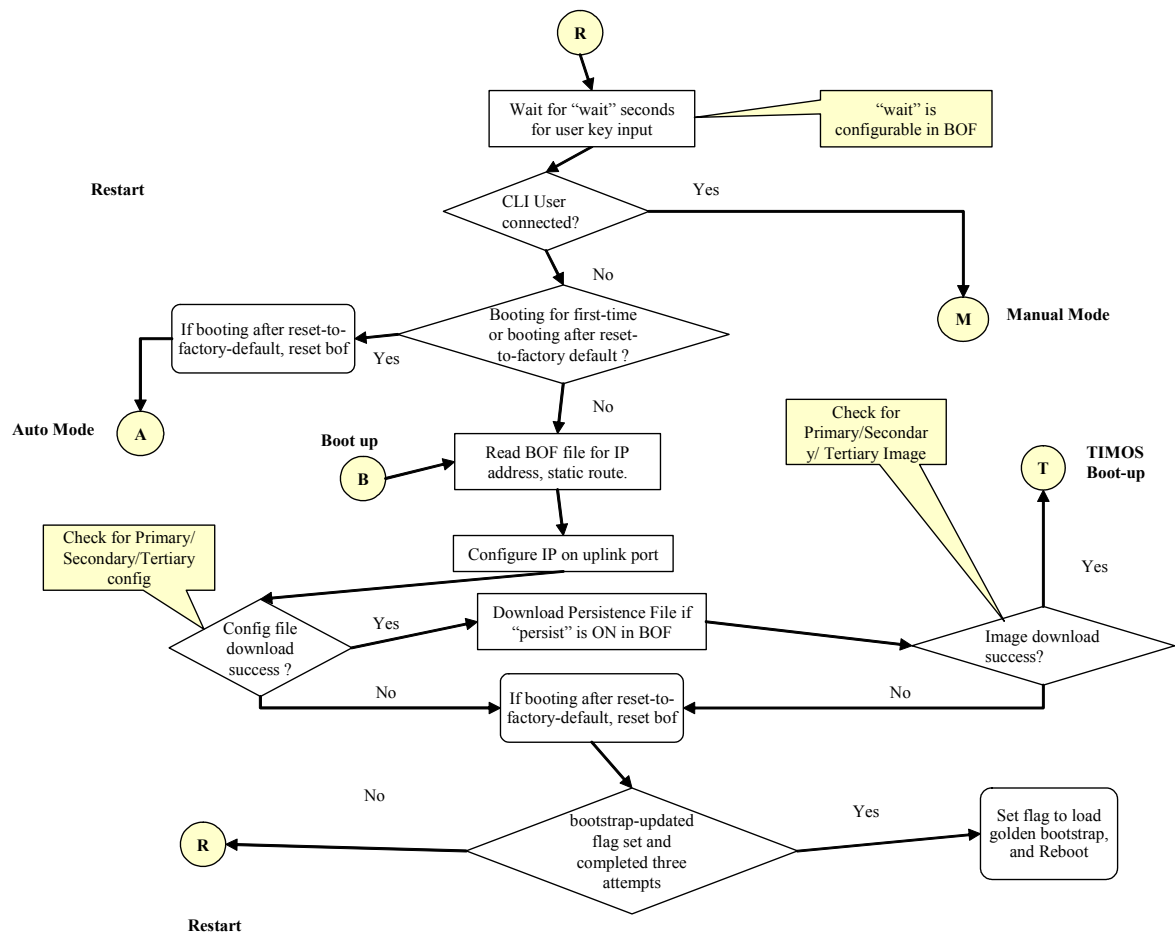
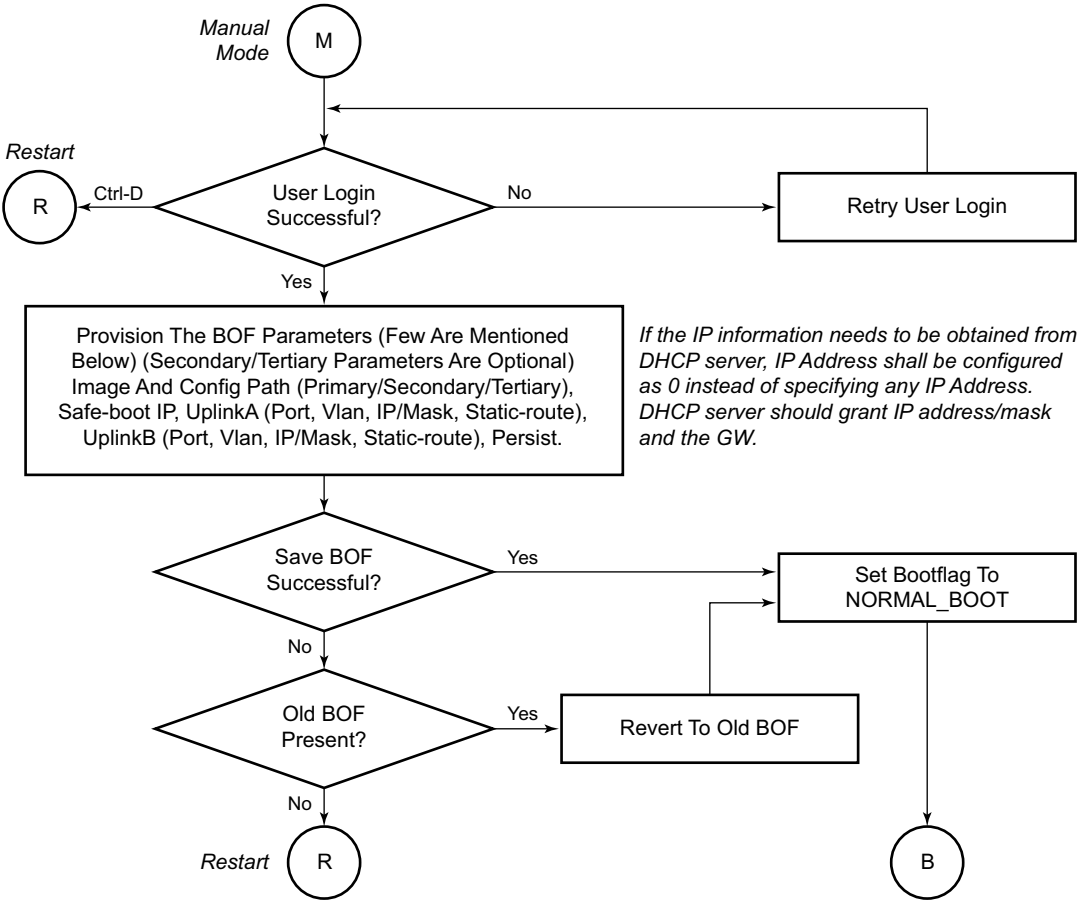


Figure 5: Bootstrap Process - System Initialization - Part II-A



OSSG284

Figure 6: Bootstrap Process - System Initialization - Part II-B

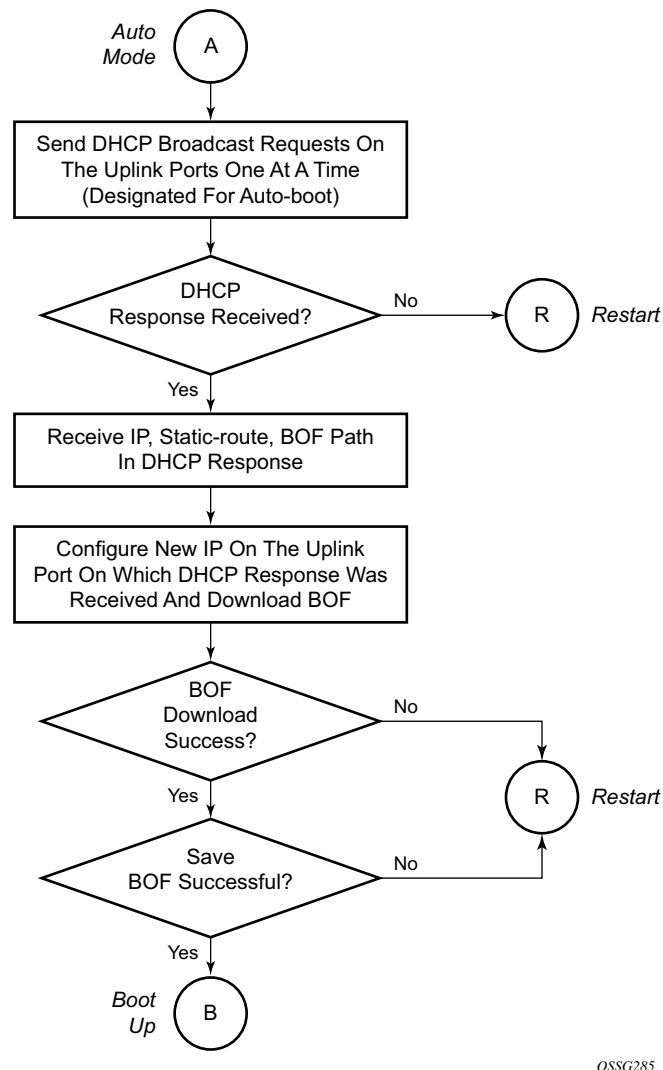


Figure 7: Bootstrap Process - System Initialization - Part II-C

When the runtime image is successfully downloaded, control is passed from the bootstrap image. The runtime image attempts to load the configurations from the downloaded configuration file. If no configuration file location is present in the BOP file, then the system is loaded with default configuration. Also during the auto-init, if the configuration file or image file download fails from the network, then the system is the auto-init procedure.

Ping Check

If the system is booted up using the auto-init procedure, the runtime image performs a ping check to make sure that the system has IP connectivity. The runtime image, after loading the configurations from the configuration file, tries three times to ping the IP address specified as the ping-address parameter in the BOF file, at a 2, 8 and 16 minutes interval minute interval. If the ping does not succeed, the system is rebooted with BOF reset after 1 minute and the whole boot process is repeated. If address in the BOF is zero or the ping address is not given, the ping check is not done. [Figure 8](#) describes the TiMos Boot — System Initialization Part III.

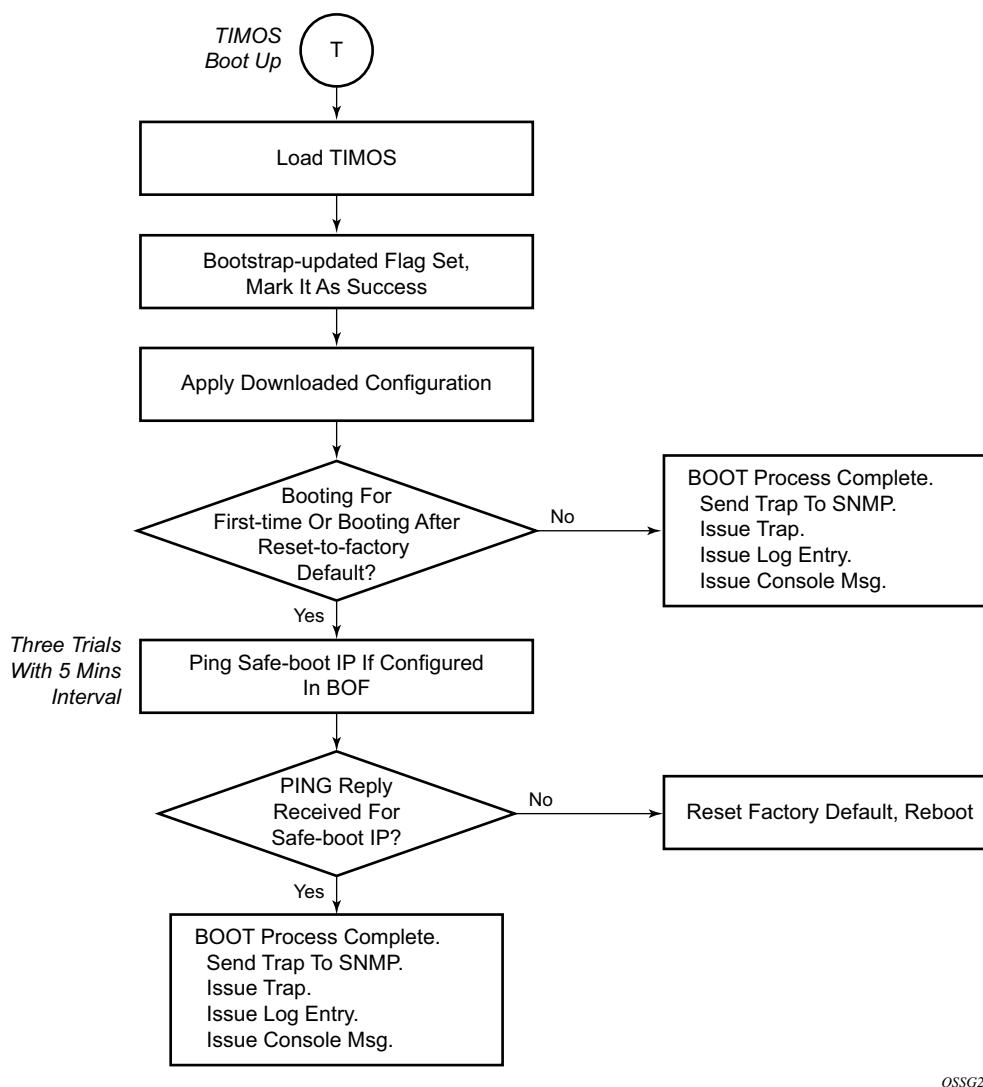


Figure 8: Timos Boot - System Initialization - Part III

Persistence

The following displays an example of BOF output for 7210 SAS-E devices.

```
*A:7210>show# bof
=====
BOF (Memory)
=====
primary-image ftp://*:135.254.170.22//import/panos_builds/nightly/0.0
/I783/STU-sultan
primary-config ftp://*:10.135.25.100/tftpboot/STU/2597-ver2.cfg
secondary-config tftp://10.135.25.100/STU/2597-ver2.cfg
#eth-mgmt Port Settings:
no eth-mgmt-disabled
eth-mgmt-address 10.135.25.91/24
eth-mgmt-route 10.135.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.250.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.254.0.0/16 next-hop 10.135.25.1
eth-mgmt-autoneg
eth-mgmt-duplex full
eth-mgmt-speed 100
#uplinkA Port Settings:
uplinkA-port 1/1/24
uplinkA-address 10.135.25.91/24
uplinkA-vlan 0
uplinkA-route 10.135.0.0/16 next-hop 10.135.25.1
uplinkA-route 135.254.0.0/16 next-hop 10.135.25.1
#uplinkB Port Settings:
uplinkB-port 1/1/2
uplinkB-address 0
uplinkB-vlan 0
#System Settings:
wait 3
persist off
console-speed 115200
no console-disabled
=====
*A:7210>show#
```

The following displays an example of BOF output for 7210 SAS D device:

```
*A:SAS-D>show# bof
=====
BOF (Memory)
=====
primary-image ftp://*:135.254.170.22//home/***/images/SASD-both.tim
primary-config cfl:\****.cfg
#uplinkA Port Settings:
uplinkA-port 1/1/10
uplinkA-address 10.135.20.152/24
uplinkA-vlan 0
uplinkA-route 10.135.0.0/16 next-hop 10.135.20.1
uplinkA-route 135.250.0.0/16 next-hop 10.135.20.1
uplinkA-route 135.254.0.0/16 next-hop 10.135.20.1
#System Settings:
```

```
wait          3
persist       off
console-speed 115200
no console-disabled

=====
*A:SAS-D>show##
```

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. 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.

Configuration guidelines for use of software images with the 128MB 7210 SAS-D platform

The new 7210 SAS-D platforms with 128MB flash can boot entirely new software releases. The older images cannot be used with the new devices. The older 7210 SAS-D platforms with 64MB flash can use any image. All new devices are shipped with the latest bootrom. The system bootrom, bootloader and Timos image introduces the following checks to prevent use of older releases with the new hardware:

- If a user issues an admin reboot upgrade with an older boot.tim, then bootrom detects and fails to load the bootloader, instead the bootrom uses the golden bootloader, loads it for booting with the bootrom and finally loads both.tim.
 - If a user issues an admin reboot upgrade with an older boot.tim, and an older both.tim, then bootrom detects and fails to load the bootloader, instead the bootrom uses the golden bootloader and stops booting as the user specifies an older version of the both.tim, which the system cannot use. This process results in loss of management connectivity.
 - If a user issues an admin reboot upgrade with an older boot.tim, an older both.tim as primary, and a newer both.tim as secondary, then the bootrom detects and fails to load the bootloader, instead the bootrom use the golden bootloader. The bootloader checks the primary location for a compatible both.tim image and as the image is an older version the boot fails. The bootloader then checks the secondary location for a compatible both.tim image and as the image is a newer version image the bootloader successfully boots the system.
 - The **admin>update-golden-bootstrap** CLI command does not update the golden-bootstrap image with the boot.tim specified in the parameter value, if the boot.tim is not a new image.
-

Out-of-band (OOB) Ethernet Management Port

Note: Out-of-band Ethernet port is not supported on 7210 SAS-D devices. The 7210 platforms support out-of-band ethernet management port for management of the node. An Out-of-band Ethernet port can be used to download the TIMOS image file and the configuration file by creating a BOF file manually. The out-of-band management port allows for use of both IPv4 and IPv6.

Please check the release notes to know the software release where support for out-of-band management port is available and for software release availability of IPv6 support.

Configuration Guidelines for use of IPv6 for out-of-band management of the node

- The management port on the management router instance only supports host functionality.
 - It is necessary to have an IPv4 address configured in the bof file. A bof file that contains only IPv6 addresses is not supported.
 - IPv6 duplicate address detection is not supported.
 - IPv6 auto-configuration is not supported.
 - IPv6 over IPv4 tunneling is not supported.
 - IPv6 path MTU discovery is not supported.
 - Router discovery option is not supported on the management port.
-

Security for Console Port and Ethernet Management Port

The 7210 OS supports disabling the console port and out-of-band Ethernet management port. In remote deployments, operators can choose to disable user access to the node through the console and through the ethernet management port to prevent unauthorised and malicious access. Operators can use the command `bof> console-disabled` to disable the console and the command `bof> eth-mgmt-disabled` to disable the use of Ethernet management port.

Note: Access to console is only disabled when the Timos image is loaded. Console access remains unchanged during boot loader stage of the boot up process.

Reset the node to factory default setting

From release 4.0 and onwards, the default BOF password can be modified by the user. To edit the BOF parameters, user needs to provide the correct password. If the user forgets the password and fails to provide a correct password after three attempts, the system prompts the user to reset the BOF password to factory default. As a security measure, to prevent a malicious user from using it to gain access to the configuration files, when the password is reset to default, the system also resets the flash to factory defaults (that is, it removes all the files from the flash except for the boot image file (`cf1:\boot.tim`) and Timos image file (`cf1:\both.tim`)) and reboots the node with the factory default settings. The node is rebooted after the password is reset, to boot up with the factory default settings. After boot up, the user needs to setup the box using the same steps as used to boot the box the first time when it was received from the factory. User can use the factory default password 'password' to edit the BOF parameters after the boot up subsequent to reboot and choose to change the password again. The bof password can be changed only in the Timos CLI.

Note 1: The BOF password can be changed from default value to any other user defined value only at the Timos level.

Note 2: It is highly recommended that user does not rename cfl:\boot.tim and cfl:\both.tim, if the system needs to retain them during the password recovery procedure. Additionally, it is highly recommended that the user takes a backup of all the image files, configuration files and other data.

The following logs show the system prompts displayed on the console when user forgets the password and chooses to reset the password to factory default setting. Also, shown are the BOF contents after and before the reset. Note that the BOF parameters are set to default after password reset.

```

TIMOS BOOT LOADER

CPLD Version: 2.1
Time from clock is FRI AUG 19 09:22:46 2011 UTC
USB:   USB EHCI 1.00
scanning bus for devices...
1 USB Device(s) found
Number of blocks in device 0 is 0
Number of bytes per block in device 0 is 0
Switching serial output to sync mode...   done

Looking for cfl:/bof.cfg ... OK, reading

Contents of Boot Options File on cfl:
    primary-image      ftp://*:~@135.250.27.40/xxx/xx/xxx/xx/xxx/both.tim
    primary-config     cfl:\sasm.cfg
#eth-mgmt Port Settings:
    no eth-mgmt-disabled
    eth-mgmt-address   10.135.20.115/24 active
    eth-mgmt-route     0.0.0.0/0 next-hop 10.135.20.1
    eth-mgmt-autoneg
    eth-mgmt-duplex    full
    eth-mgmt-speed     100
#uplinkA Port Settings:
    uplinkA-port       1/1/1
    uplinkA-address    0
    uplinkA-vlan        0
#uplinkB Port Settings:
    uplinkB-port       1/1/2
    uplinkB-address    0
    uplinkB-vlan        0
#System Settings:
    wait               3
    persist            off
    console-speed      115200
    uplink-mode        network
    acl-mode           IPv6-None
    use-expansion-card-type m4-ds1-ces
    no console-disabled

Hit a key within 3 seconds to change boot parameters...

Enter password to edit the Boot Options File
Or CTRL-D to exit the prompt

Password:
Incorrect password

```

Configuration and Image Loading

```
Password:
Incorrect password

Password:
Incorrect password

Authentication failed, Do you want to reset password?(yes/no)

*****
On reset,the node's flash contents will be set to factory defaults.
All files on the flash will be removed. If present, files
cfl:/boot.tim and cfl:/both.tim are not removed.
Please ensure that you have a backup of the required
files before you proceed.
*****

'yes' or 'no' ?
'yes' or 'no' ? yes

*****
*** Chassis must not be powered off nor ***
*** cards removed while password reset ***
*** is in progress ***
*****
Password reset complete. Restarting...
```

At this point the password has been reset and the node is rebooted to boot up with factory default settings.

```
Resetting...OK
Ø
Alcatel-Lucent 7210 Boot ROM. Copyright 2009-2011 Alcatel-Lucent.

All rights reserved. All use is subject to applicable license agreements.
Running POST tests from ROM
Testing ROM load area...done

Relocating code...Jumping to RAM

Performing second stage RAM test....passed

Board Serial Number is 'NS1023C1436'
Bootlog started for Version 9-V-0.0.I1111
Build V-0.0.I1111 bootrom/mpc 7xxx
Built on Wed Jun 29 21:55:30 IST 2011 by builder in /builder/0.0/panos/main

?Attempting to load from file cfl:/boot.tim
Version L-4.0.beta-private, Sat Aug 20 12:59:26 IST 2011 by abc /abc/ws-40b/panos/main
text:(3706043-->13139264) + data:(528557-->2068192)
Starting at 0xb000000...

Total Memory: 1GB Chassis Type: sas Card Type: badami_7210
TiMOS-L-4.0.beta-private boot/mpc ALCATEL SAS 7210 Copyright (c) 2000-2011 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Sat Aug 20 12:59:26 IST 2011 by abc in /abc/ws-40b/panos/main
```

```

TiMOS BOOT LOADER

CPLD Version: 2.1
Time from clock is FRI AUG 19 09:24:05 2011 UTC
USB:  USB EHCI 1.00
scanning bus for devices...
1 USB Device(s) found
Number of blocks in device 0 is 0
Number of bytes per block in device 0 is 0
Switching serial output to sync mode...  done

Looking for cfl:/bof.cfg ... not found
Could not find bof.cfg on any of the local drives.

Default Settings
-----
#eth-mgmt Port Settings:
    eth-mgmt-disabled
#uplinkA Port Settings:
    uplinkA-port      1/1/1
    uplinkA-address   0
    uplinkA-vlan      0
#uplinkB Port Settings:
    uplinkB-port      1/1/2
    uplinkB-address   0
    uplinkB-vlan      0
#System Settings:
    wait              3
    persist            off
    console-speed     115200
    uplink-mode        network
    acl-mode           IPv6-None
    use-expansion-card-type  m4-ds1-ces
    no console-disabled
Hit a key within 1 second to change boot parameters...
Enter password to edit the Boot Options File
Or CTRL-D to exit the prompt
Password:

```

Note: At this prompt, the default password “password” must be used.

Initial System Startup Process Flow

Figure 9 displays the process start your system. Note that this example assumes that the boot loader and BOF image and configuration files are successfully located.

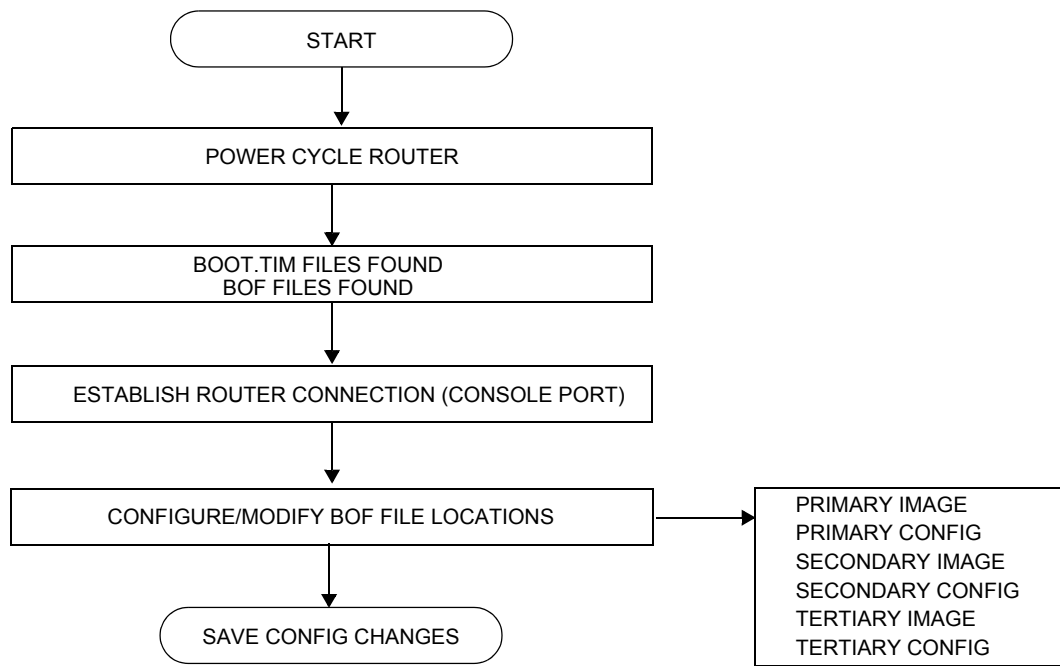


Figure 9: System Startup Process Flow

Configuration Notes

This section describes BOF configuration caveats.

- 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.

Configuring Boot File Options with CLI

This section provides information to configure BOF parameters with CLI.

Topics in this section include:

- [Configuring Boot File Options with CLI on page 129](#)
- [BOF Configuration Overview on page 130](#)
- [Basic BOF Configuration on page 131](#)
- [Common Configuration Tasks on page 133](#)
- [Configuring BOF Parameters on page 139](#)
- [Service Management Tasks on page 140](#)
 - [Viewing the Current Configuration on page 140](#)
 - [Modifying and Saving a Configuration on page 142](#)
 - [Saving a Configuration to a Different Filename on page 145](#)
 - [Rebooting on page 145](#)

BOF Configuration Overview

Alcatel-Lucent routers do not contain a boot EEPROM. The bootstrap image is loaded from the boot.tim file. The BOF file performs the following tasks:

1. Sets up the uplink ports (speed, duplex, auto).
2. Assign the IP address (either statically or using DHCP) for the uplink port.
3. Assign the VLAN to the uplink port.
4. Create static routes for the uplink routes.
5. Sets the console port speed.
6. Configures the Domain Name System (DNS) name and DNS servers.
7. Configures the primary, secondary, tertiary configuration source.
8. Configures the primary, secondary, and tertiary image source.
9. Configures operational parameters.

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:

- Uplink port parameters
- Primary image location
- Primary configuration location

Following is a sample of a basic BOF configuration for 7210 SAS-E devices.

```
*A:7210>show# bof
=====
BOF (Memory)
=====
primary-image ftp://*:~@135.254.170.22//import/panos_builds/nightly/0.0
/I783/STU-sultan
primary-config ftp://*:~@10.135.25.100/tftpboot/STU/2597-ver2.cfg
secondary-config tftp://10.135.25.100/STU/2597-ver2.cfg
#eth-mgmt Port Settings:
no eth-mgmt-disabled
eth-mgmt-address 10.135.25.91/24
eth-mgmt-route 10.135.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.250.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.254.0.0/16 next-hop 10.135.25.1
eth-mgmt-autoneg
eth-mgmt-duplex full
eth-mgmt-speed 100
#uplinkA Port Settings:
uplinkA-port 1/1/24
uplinkA-address 10.135.25.91/24
uplinkA-vlan 0
uplinkA-route 10.135.0.0/16 next-hop 10.135.25.1
uplinkA-route 135.254.0.0/16 next-hop 10.135.25.1
#uplinkB Port Settings:
uplinkB-port 1/1/2
uplinkB-address 0
uplinkB-vlan 0
#System Settings:
wait 3
persist off
console-speed 115200
no console-disabled
=====
*A:7210>show#
```

The following displays an example of BOF output for 7210 SAS D device:

```
*A:SAS-D>show# bof
=====
BOF (Memory)
```

Basic BOF Configuration

```
=====
primary-image      ftp://*:135.254.170.22//home/***/images/SASD-both.tim
primary-config     cfl:\****.cfg
#uplinkA Port Settings:
uplinkA-port       1/1/10
uplinkA-address    10.135.20.152/24
uplinkA-vlan       0
uplinkA-route      10.135.0.0/16 next-hop 10.135.20.1
uplinkA-route      135.250.0.0/16 next-hop 10.135.20.1
uplinkA-route      135.254.0.0/16 next-hop 10.135.20.1
#System Settings:
wait               3
persist            off
console-speed      115200
no console-disabled
=====
*A:SAS-D>show#
```

Common Configuration Tasks

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

- [Searching for the BOF on page 134](#)
 - [Accessing the CLI on page 137](#)
 - [Console Connection on page 137](#)
- [Configuring BOF Parameters on page 139](#)

For details about hardware installation and initial router connections, refer to the specific hardware installation guide.

Searching for the BOF

The BOF should be on the same drive as the bootstrap image file. If the system cannot load or cannot find the BOF, then the system checks whether the boot sequence was manually interrupted else continues with the auto-init mode. The system prompts for a different image and configuration location.

The following example displays an example of the output when the boot sequence is interrupted for 7210 SAS-E devices.

```
Hit a key within 3 seconds to change boot parameters...
```

```
Enter password to edit the Boot Options File
Or CTRL-D to exit the prompt
```

```
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.
"reset"   - reset the bof and reboot.
```

```
Press ENTER to begin, or 'flash' to enter firmware update, or the shell password...
```

```
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
```

```
cfl:/timos1.0R1
ftp://user:passwd@192.168.1.150/./timos1.0R1
ftp://user:passwd@[3FFE::1]/./timos1.0R1
tftp://192.168.1.150/./timos1.0R1
tftp://3FFE::1/./timos1.0R1
```

```
The existing Image URL is 'ftp://*:~@10.10.170.22//home/****/images/both.tim'
```

```
Press ENTER to keep it.
```

```
Software Image URL:
```

```
Using: 'ftp://*:~@10.10.170.22//home/****/images/both.tim'
```

```
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
```

```
cfl:/config.cfg
ftp://user:passwd@192.168.1.150/./config.cfg
ftp://user:passwd@[3FFE::1]/./config.cfg
tftp://192.168.1.150/./config.cfg
tftp://3FFE::1/./config.cfg
```

The existing Config URL is 'ftp://*:10.135.25.100/tftpboot/STU/config.cfg'
 Press ENTER to keep it, or the word 'none' for no Config URL.
 Config File URL: none

Network Configuration

Boot Interface Management

You specified a network location for either the software or the configuration file. You need to configure either eth-mgmt or uplinkA or uplinkB ports. You will be asked to configure the port number, IP address, static routes, and VLAN Id in case of uplink ports.

eth-mgmt Port Setting

Existing eth-mgmt port settings are:

```
eth-mgmt-port
eth-mgmt-address    10.135.25.97/24
eth-mgmt-route      10.135.0.0/16 next-hop 10.135.25.1
eth-mgmt-route      135.254.0.0/16 next-hop 10.135.25.1
```

eth-mgmt port is configured for Boot Interface Management,
 Press ENTER to proceed with existing port settings
 Or "disable" to disable the port for Boot Interface Management
 Or "edit" to change the port settings:

uplinkA Port Setting

Existing uplinkA port settings are:

```
uplinkA-port        1/1/24
uplinkA-address     0
uplinkA-vlan        0
```

uplinkA port is configured for Boot Interface Management,
 Press ENTER to proceed with existing port settings
 Or "disable" to disable the port for Boot Interface Management
 Or "edit" to change the port settings:

uplinkB Port Setting

Existing uplinkB port settings are:

```
uplinkB-port        1/1/2
uplinkB-address     0
uplinkB-vlan        0
```

uplinkB port is configured for Boot Interface Management,
 Press ENTER to proceed with existing port settings
 Or "disable" to disable the port for Boot Interface Management
 Or "edit" to change the port settings:

New Settings

Common Configuration Tasks

```
-----
primary-image      ftp://*:135.254.170.22//home/****/images/both.tim
secondary-config   tftp://10.135.25.100/STU/config.cfg
#eth-mgmt Port Settings:
no eth-mgmt-disabled
eth-mgmt-address   10.135.25.97/24
eth-mgmt-route     10.135.0.0/16 next-hop 10.135.25.1
eth-mgmt-route     135.254.0.0/16 next-hop 10.135.25.1
eth-mgmt-autoneg
eth-mgmt-duplex    full
eth-mgmt-speed     100
#uplinkA Port Settings:
uplinkA-port       1/1/24
uplinkA-address    0
uplinkA-vlan       0
#uplinkB Port Settings:
uplinkB-port       1/1/2
uplinkB-address    0
uplinkB-vlan       0
#System Settings:
wait               3
persist            off
console-speed      115200
no console-disabled
```


Accessing the CLI

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

- When the power to the chassis is turned on, the 7210 SAS 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).
-

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 connector for connecting to a RS232 port (provides a RJ45 connector).

Table 14: Console Configuration Parameter Values

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

[Figure 10](#) displays an example of the Console port on a 7210 SAS E front panel.

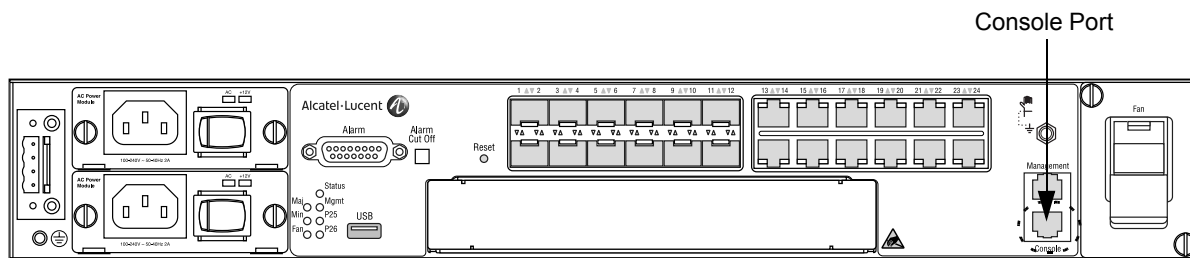


Figure 10: 7210 SAS E Front Panel Console Port

Figure 11 displays an example of the Console port on a 7210 SAS D front panels.

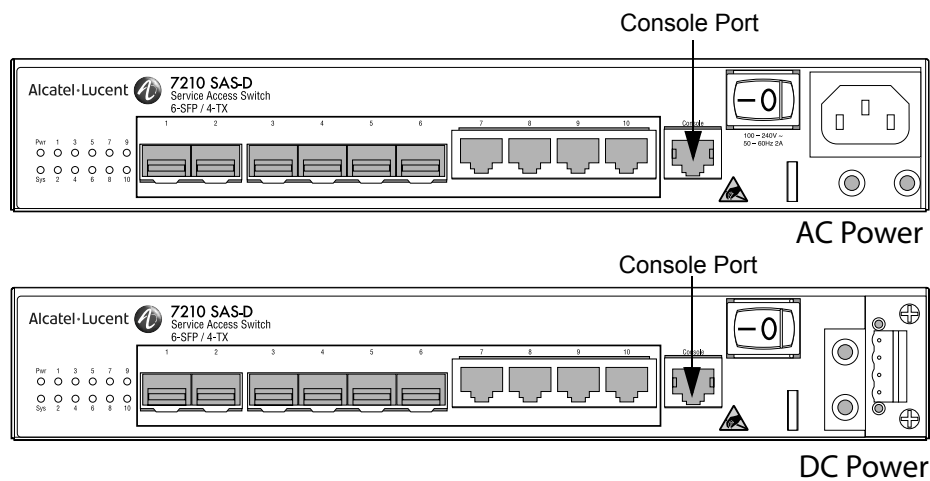


Figure 11: 7210 SAS D Front Panel Console Port

To establish a console connection:

- Step 1** Connect the terminal to the Console port on the front panel 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.

Configuring BOF Parameters

The following output displays a BOF configuration for 7210 SAS-E:

```
*A:7210>show# bof
=====
BOF (Memory)
=====
primary-image ftp://*:~@135.254.170.22//import/panos_builds/nightly/0.0
/I783/STU-sultan
primary-config ftp://*:~@10.135.25.100/tftpboot/STU/2597-ver2.cfg
secondary-config tftp://10.135.25.100/STU/2597-ver2.cfg
#eth-mgmt Port Settings:
no eth-mgmt-disabled
eth-mgmt-address 10.135.25.91/24
eth-mgmt-route 10.135.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.250.0.0/16 next-hop 10.135.25.1
eth-mgmt-route 135.254.0.0/16 next-hop 10.135.25.1
eth-mgmt-autoneg
eth-mgmt-duplex full
eth-mgmt-speed 100
#uplinkA Port Settings:
uplinkA-port 1/1/24
uplinkA-address 10.135.25.91/24
uplinkA-vlan 0
uplinkA-route 10.135.0.0/16 next-hop 10.135.25.1
uplinkA-route 135.254.0.0/16 next-hop 10.135.25.1
#uplinkB Port Settings:
uplinkB-port 1/1/2
uplinkB-address 0
uplinkB-vlan 0
#System Settings:
wait 3
persist off
console-speed 115200
console-disabled
=====
*A:7210>show#
```

Service Management Tasks

This section discusses the following service management tasks:

- [System Administration Commands on page 140](#)
 - [Viewing the Current Configuration on page 140](#)
 - [Modifying and Saving a Configuration on page 142](#)
 - [Deleting BOF Parameters on page 143](#)
 - [Saving a Configuration to a Different Filename on page 145](#)
-

System Administration Commands

Use the following administrative commands to perform management tasks.

CLI Syntax: A:ALA-1# admin
check-golden-bootstrap
debug-save [<file-url>]
disconnect [address <ip-address> | username <user-name> |
{console|telnet|ftp|ssh}]
display-config
[no]enable-tech
reboot [auto-init][now]
save [file-url] [detail] [index]
set-time <date> <time>
tech-support <file-url>
update-golden-bootstrap [file-url]

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 displays an example of a configuration file:

```
*A:sim169# admin display-config
# TiMOS-B-0.0.I218 both/i386 ALCATEL SAS-E 7210 Copyright (c) 2000-2008 Alcatel-
Lucent.
# All rights reserved. All use subject to applicable license agreements.
```

```
# Built on Fri Sep 26 20:46:58 IST 2008 by panosbld in /panosbld/ws/panos/main

# Generated THU JUN 23 19:19:22 2005 UTC

exit all
configure
#-----
echo "System Configuration"
#-----
    system
        name "7210-3"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        ccm 1
        exit
        snmp
        exit
        login-control
            idle-timeout 1440
            motd text "7210-3"
        exit
        time
            sntp
            shutdown
            exit
            zone UTC
        exit
        thresholds
            rmon
            exit
        exit
    exit...
...
#-----

# Finished FRI Nov 21 15:06:16 2008 UTC
A:*A:sim169##
```

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 cf1:
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 cf1:\test123.cfg
Saving config.# Saved to cf1:\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.

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 the BOF file and then rebooting, causes the system to enter auto mode.

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 cfl:
A:ALA-1>bof#
```

The following is the CLI Syntax for 7210 SAS-E:

CLI Syntax: `*A:7210>bof#`

```
no    console-speed
no    dns-domain
no    eth-mgmt-address
no    eth-mgmt-autoneg
no    eth-mgmt-disable
      eth-mgmt-duplex
no    eth-mgmt-route
      eth-mgmt-speed
      persist
no    ping-address
no    primary-config
no    primary-dns
no    primary-image
      save
no    secondary-config
no    secondary-dns
no    secondary-image
no    tertiary-config
no    tertiary-dns
no    tertiary-image
no    uplinkA-address
no    uplinkA-port
no    uplinkA-route
no    uplinkA-vlan
no    uplinkB-address
no    uplinkB-port
```

```
no    uplinkB-route
no    uplinkB-vlan
wait
```

The following is the CLI Syntax for 7210 SAS-D:

CLI Syntax: *A:7210>bof#

```
no console-speed
no dns-domain
persist
no ping-address
no primary-config
no primary-dns
no primary-image
save
no secondary-config
no secondary-dns
no secondary-image
no tertiary-config
no tertiary-dns
no tertiary-image
no uplinkA-address
no uplinkA-port
no uplinkA-route
no uplinkA-vlan
no uplinkB-address
no uplinkB-port
no uplinkB-route
no uplinkB-vlan
wait
```


Saving a Configuration to a Different Filename

Save the current configuration with a unique filename to have additional backup copies and to edit parameters with a text editor. You can save your current configuration to an ASCII file.

Use either of the following CLI syntax to save a configuration to a different location:

CLI Syntax: `bof# save [cflash-id]`

Example:

```
A:ALA-1# bof
A:ALA-1>bof# save cfl:
A:ALA-1>bof#
```

or

CLI Syntax: `admin# save [file-url] [detail] [index]`

Example:

```
A:ALA-1>admin# save cfl:\testABC.cfg
Saving config.# Saved to cfl:\testABC.cfg
... complete
A:ALA-1#
```

Rebooting

When an **admin>reboot** command is issued, the system reboots. Changes are lost unless the configuration is saved. Use the **admin>save file-url** command to save the current configuration. The user is prompted to confirm the reboot operation. If the now option is not specified, the user is prompted to confirm the reboot operation.

Use the following CLI syntax to reboot:

CLI Syntax: `admin# reboot [auto-init][now]`

Example:

```
A:ALA-1>admin# reboot
A:DutA>admin# reboot

Are you sure you want to reboot (y/n)? y
```

Resetting...OK

```
Alcatel-Lucent 7210 Boot ROM. Copyright 2000-2009 Alcatel-Lucent.
All rights reserved. All use is subject to applicable license agreements.
Running POST tests from ROM
Testing ROM load area...done
```

Relocating code...Jumping to RAM

...

When an **admin reboot auto-init** command is issued, the system resets the existing BOF file and reboots. The system startup process after the **admin reboot auto-init** command is executed is the same as the first time system boot as described in [System Initialization on page 108](#).

NOTE: Since the BOF is reset, the system may not boot up with the last saved system configuration unless the new BOF file also uses the same configuration file. If it is required that the system boot up with the last saved system configuration, it is recommended to use the **admin>save file-url** command to save the current system configuration and modify the BOF to use this.

Use the following CLI to reset the BOF and reboot:

CLI Syntax: admin# reboot auto-init [now]

Example: *A:ALA-1# admin reboot auto-init

WARNING: Configuration and/or Boot options may have changed since the last save.

Are you sure you want to reset the bof and reboot (y/n)? Y

Resetting...OK

Alcatel-Lucent 7210 Boot ROM. Copyright 2000-2008 Alcatel-Lucent.

All rights reserved. All use is subject to applicable license agreements.

BOF Command Reference

Command Hierarchies

Configuration Commands

bof

- **bof-password**
- **[no] console-disabled**
- **console-speed** *baud-rate*
- **no console-speed**
- **dns-domain** *dns-name*
- **no dns-domain**
- **[no] eth-mgmt-address** *ip-prefix/ip-prefix-length* (Not supported on 7210 SAS-D)
- **[no] eth-mgmt-autoneg** (Not supported on 7210 SAS-D)
- **[no] eth-mgmt-address** (Not supported on 7210 SAS-D)
- **[no] eth-mgmt-disabled** (Not supported on 7210 SAS-D)
- **eth-mgmt-duplex** {**full** | **half**} (Not supported on 7210 SAS-D)
- **[no] eth-mgmt-route** *ip-prefix/ip-prefix-length*
- **next-hop** *ip-address* (Not supported on 7210 SAS-D)
- **eth-mgmt-speed** *speed* (Not supported on 7210 SAS-D)
- **persist** {**on** | **off**}
- **ping-address** *ip-address*
- **no ping-address**
- **primary-config** *file-url*
- **no primary-config**
- **primary-dns** *ip-address*
- **no primary-dns**
- **primary-image** *file-url*
- **no primary-image**
- **save** [*cflash-id*]
- **secondary-config** *file-url*
- **no secondary-config**
- **[no] secondary-dns** *ip-address*
- **secondary-image** *file-url*
- **no secondary-image**
- **tertiary-config** *file-url*
- **no tertiary-config**
- **tertiary-dns** *ip-address*
- **no tertiary-dns**
- **tertiary-image** *file-url*
- **no tertiary-image**
- **wait** *seconds*
- **uplinkA-address** *ip-address/mask*
- **no uplinkA-address**
- **uplinkA-port** *port-id*
- **no uplinkA-port**
- **[no] uplinkA-route** *ip-address/mask next-hop ip-address*
- **uplinkA-vlan** *0..4094*
- **no uplinkA-vlan**
- **uplinkB-address** *ip-address/mask*

BOF Command Reference

- **no uplinkB-address**
- **uplinkB-port** *port-id*
- **no uplinkB-port**
- [**no**] **uplinkB-route** *ip-address/mask* **next-hop** *ip-address*
- **uplinkB-vlan** *0..4094*
- **no uplinkB-vlan**
- **wait** *seconds*

Show Commands

- show**
 - **bof** [*cflash-id* | **booted**]
 - **boot-messages**

Configuration Commands

File Management Commands

bof

Syntax	bof
Context	<ROOT>
Description	This command creates or edits the boot option file (BOF) for the specified local storage device. A BOF file specifies where the system searches for runtime images, configuration files, and other operational parameters during system initialization. BOF parameters can be modified. Changes can be saved to a specified compact flash. The BOF must be located in the root directory of either an internal or external compact flash local to the system and have the mandatory filename of <i>bof.cfg</i>. When modifications are made to in-memory parameters that are currently in use or operating, the changes are effective immediately. For example, if the console-speed is changed, the change takes place immediately. Only one entry of the BOF configuration command statement can be saved once the statement has been found to be syntactically correct. No default boot option file exists.
Default	none

save

Syntax	save [<i>cf-flash-id</i>]
Context	bof
Description	This command uses the boot option parameters currently in memory and writes them from the boot option file to the compact flash. The BOF is located in the root directory of the internal compact flash drive local to the system and have the mandatory filename of <i>bof.cfg</i>. Command usage: • bof save — Saves the BOF to the flash drive CF1: • bof save cf1: — Saves the BOF to cf1:
Default	Saves must be explicitly executed. The BOF is saved to cf1: if a location is not specified.

Parameters *flash-id* — The compact flash ID where the *bof.cfg* is to be saved.

Values cfl

Default cfl

BOF Processing Control

wait

Syntax	wait <i>seconds</i>		
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	3		
Parameters	<i>seconds</i> — The time to pause at the start of the boot process, in seconds. <table><tr><td>Values</td><td>1 — 10</td></tr></table>	Values	1 — 10
Values	1 — 10		

Console Port Configuration

bof-password

Syntax	bof-password <i>password</i>
Context	bof
Description	This command allows the user to configure a BOF password. The user will have to provide this password to edit the BOF parameters in the boot loader. It also implements a mechanism for password recovery, if the user forgets the password. If the user forgets the password, it can be reset to factory default. As a security measure, to prevent a malicious user for using it gain access to the configuration files, when the password is reset to default, the system also resets the flash to factory defaults (that is, it removes all the files from the flash except for the boot image file (cf1:\boot.tim) and Timos image file (cf1:\both.tim)) and reboots the node with the factory default settings. After boot up, the user needs to setup the box using the same steps as used to boot the box the first time when it was received from the factory. User can use the factory default password 'password' to edit the BOF parameters after the boot up subsequent to reboot and choose to change the password again. NOTE: It is highly recommended that user does not rename cf1:\boot.tim and cf1:\both.tim, if the system needs to retain them during the password recovery procedure. Additionally, it is highly recommended that the user takes a backup of all the image files, configuration files and other data.
Default	The factory default password is 'password'
Parameters	<i>password</i> — Specifies the bof password.
	Values Maximum of 20 characters.

console-disabled

Syntax	[no] console-disabled
Context	bof
Description	This command allows the user to enable or disable the serial port console for use. In remote deployments this command provides additional security mechanism for the user. The console can be disabled to prevent unauthorized access to the system. Note: Console is always available for use when the device is booting up. This command is applicable only after the Timos image [SROS] (that is the both.tim) is up and running successfully. If the user executes this command in the BOF CLI context, the command takes effect only during the next boot. A BOF Save operation must be performed after executing the console-disabled command. The no form of the command enables the console. This is the default value.
Default	no console-disabled

console-speed

Syntax	console-speed <i>baud-rate</i> no console-speed
Context	bof
Description	This command configures the console port baud rate. When this command is issued while editing the BOF file used for the most recent boot, both the BOF file and the active configuration are changed immediately. The no form of the command reverts to the default value.
Default	115200 — console configured for 115,200 bps operation
Parameters	<i>baud-rate</i> — The console port baud rate, expressed as a decimal integer.
	Values 9600, 19200, 38400, 57600, 115200

Image and Configuration Management

persist

Syntax	persist {on off}
Context	bof
Description	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, etc. This reduces resynchronizations of the Network Management System (NMS) with the affected network element. 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. Notes: • 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	off
Parameters	<i>on</i> — Create when saving the configuration. <i>off</i> — Disables the system index saves between reboots.

primary-config

Syntax	primary-config <i>file-url</i> 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. Note that 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	none		
Parameters	<i>file-url</i> — The primary configuration file location, expressed as a file URL.		
	Values	file-url	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
		local-url	[<cf-flash-id/> <usb-flash-id>][<i>file-path</i>]
		remote-url	[{ftp:// tftp://} <i>login:pswd@remote-locn/</i>][<i>file-path</i>]
		cf-flash-id	cf1:
		usb-flash-id	uf1:

primary-image

Syntax	primary-image <i>file-url</i> no primary image		
Context	bof		
Description	This command specifies the primary directory location for runtime image file loading. The system attempts to load all runtime image files configured in the primary-image first. If this fails, the system attempts to load the runtime images from the location configured in the secondary-image. If the secondary image load fails, the tertiary image specified in tertiary-image is used. The no form of the command removes the primary-image configuration.		
Default	none		
Parameters	<i>file-url</i> — The <i>location-url</i> can be either local (this flash) or a remote FTP server.		
	Values	file-url	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
		local-url	[<cf-flash-id/> <usb-flash-id>][<i>file-path</i>]
		remote-url	[{ftp:// tftp://} <i>login:pswd@remote-locn/</i>][<i>file-path</i>]
		cf-flash-id	cf1:
		usb-flash-id	uf1:

secondary-config

Syntax	secondary-config <i>file-url</i> no secondary-config		
Context	bof		
Description	This command specifies the name and location of the secondary configuration file. The system attempts to use the configuration as specified in secondary-config if the primary config cannot be located. If the secondary-config file cannot be located, the system attempts to obtain the configuration from the location specified in the tertiary-config. 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	none		
Parameters	<i>file-url</i> — The secondary configuration file location, expressed as a file URL.		
	Values	file-url	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
		local-url	[< <i>cflash-id</i> /> < <i>usb-flash-id</i> >][<i>file-path</i>]
		remote-url	[{ <i>ftp://</i> <i>tftp://</i> } <i>login:pswd@remote-locn/</i>][<i>file-path</i>]
		cflash-id	<i>cf1</i> :
		usb-flash-id	<i>ufl</i> :

secondary-image

Syntax	secondary-image <i>file-url</i> no secondary-image		
Context	bof		
Description	This command specifies the secondary directory location for runtime image file loading. The system attempts to load all runtime image files configured in the primary-image first. If this fails, the system attempts to load the runtime images from the location configured in the secondary-image. If the secondary image load fails, the tertiary image specified in tertiary-image is used. The no form of the command removes the secondary-image configuration.		
Default	none		
Parameters	<i>file-url</i> — The <i>file-url</i> can be either local (this local flash) or a remote FTP server.		
	Values	file-url	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
		local-url	[< <i>cflash-id</i> /> < <i>usb-flash-id</i> >][<i>file-path</i>]
		remote-url	[{ <i>ftp://</i> <i>tftp://</i> } <i>login:pswd@remote-locn/</i>][<i>file-path</i>]
		cflash-id	<i>cf1</i> :
		usb-flash-id	<i>ufl</i> :

tertiary-config

Syntax	tertiary-config <i>file-url</i> no tertiary-config		
Context	bof		
Description	This command specifies the name and location of the tertiary configuration file. The system attempts to use the configuration specified in tertiary-config if both the primary and secondary config files cannot be located. If this file cannot be located, the system boots with the factory default configuration. Note that if an error in the configuration file is encountered, the boot process aborts. The no form of the command removes the tertiary-config configuration.		
Default	none		
Parameters	<i>file-url</i> — The tertiary configuration file location, expressed as a file URL.		
	Values	local-url	[<cf-flash-id/> <usb-flash-id>][file-path]
		cf-flash-id	cf1:
		usb-flash-id	uf1:
		remote-url	[{ftp:// tftp://} login:pswd@remote-locn/][file-path]local-url

tertiary-image

Syntax	tertiary-image <i>file-url</i> no tertiary-image		
Context	bof		
Description	This command specifies the tertiary directory location for runtime image file loading. The system attempts to load all runtime image files configured in the primary-image first. If this fails, the system attempts to load the runtime images from the location configured in the secondary-image. If the secondary image load fails, the tertiary image specified in tertiary-image is used. The no form of the command removes the tertiary-image configuration.		
Default	none		
Parameters	<i>file-url</i> — The location-url can be either local (this flash) or a remote FTP server.		
	Values	file-url	[<i>local-url</i> <i>remote-url</i>] (up to 180 characters)
		local-url	[<cf-flash-id/> <usb-flash-id>][file-path]
		remote-url	[{ftp:// tftp://} login:pswd@remote-locn/][file-path]
		cf-flash-id	cf1:
		usb-flash-id	uf1:

ping-address

Syntax	ping-address <i>ip-address</i> no ping-address
Context	bof
Description	This command specifies the IP address which would be used for ping-test after the system boots. The no form of the command removes the ping-address configuration. Setting a value of 0 also removes the ping-address configuration.
Default	none
Parameters	<i>ip-address</i> — Specifies an IPv4 ip-address in the form a.b.c.d, for example, 10.1.2.10.

uplinkA-address

Syntax	uplinkA-address <i>ip-address/mask</i> no uplinkA-address
Context	bof
Description	This command configures the uplink-A address. The no form of the command sets the uplinkA to use DHCP to get the IP and the show bof value reflects 0 for this parameter.
Parameters	<i>ip-address</i> — The IP address of the Boot Option File (BOF). This address must be unique within the subnet and specified in dotted decimal notation. <i>mask</i> — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the <i>ip-addr</i> from the <i>mask-length</i> parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Values 1 — 30

uplinkB-address

Syntax	uplinkB-address <i>ip-address/mask</i> no uplinkB-address
Context	bof
Description	This command configures the uplink-B address. The no form of the command sets the uplinkB to use DHCP to get the IP and the show bof value reflects 0 for this parameter.

Parameters	<i>ip-address</i> — The IP address of the Boot Option File (BOF). This address must be unique within the subnet and specified in dotted decimal notation. <i>mask</i> — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the <i>ip-addr</i> from the <i>mask-length</i> parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Values 1 — 30
-------------------	---

uplinkA-port

Syntax	uplinkA-port <i>port-id</i> no uplinkA-port
Context	bof
Description	This command configures the primary port to be used for boot up. The no form of the command removes all the uplinkA parameters from the BOF.
Parameters	<i>port-id</i> — Specifies the primary port to be used for boot up in the <i>slot/mda/port</i> format.

uplinkB-port

Syntax	uplinkB-port <i>port-id</i> no uplinkB-port
Context	bof
Description	This command configures the secondary port to be used for boot up. The no form of the command removes all the uplinkB parameters from the BOF.
Parameters	<i>port-id</i> — Specifies the secondary port to be used for boot up in the <i>slot/mda/port</i> format.

uplinkA-route

Syntax	[no] uplinkA-route <i>ip-address/mask next-hop ip-address</i>
Context	bof
Description	This command configures an uplink-A static route.
Parameters	<i>ip-address</i> — The IP address of the Boot Option File (BOF). This address must be unique within the subnet and specified in dotted decimal notation.

mask — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-addr* from the *mask-length* parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address.

Values 0 — 32

next-hop *ip-address* — The next hop IP address used to reach the destination.

uplinkB-route

Syntax [no] **uplinkB-route** *ip-address/mask* **next-hop** *ip-address*

Context bof

Description This command configures an uplink-B static route.

Parameters *ip-address* — The IP address of the Boot Option File (BOF). This address must be unique within the subnet and specified in dotted decimal notation.

mask — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-addr* from the *mask-length* parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address.

Values 0 — 32

next-hop *ip-address* — The next hop IP address used to reach the destination.

uplinkA-vlan

Syntax **uplinkA-vlan** 0..4094
no uplinkA-vlan

Context bof

Description This command specifies a VLAN ID to be used on uplink-A.
The **no** form of the command is used to send untagged packets on uplink-A.

uplinkB-vlan

Syntax **uplinkB-vlan** 0..4094
no uplinkA-vlan

Context bof

Description This command specifies a VLAN ID to be used on uplink-B.

The **no** form of the command is used to send untagged packets on uplink-B.

eth-mgmt-address

Note: This command is not supported on 7210 SAS-D devices.

Syntax	[no] eth-mgmt-address <i>ip-prefix\ip-prefix-length</i>
Context	bof
Description	This command assigns an IP address to the management Ethernet port in the running configuration and the Boot Option File (BOF). Deleting a BOF address entry is not allowed from a telnet session. The no form of the command deletes the IP address assigned to the Ethernet port.
Default	no eth-mgmt-address — There are no IP addresses assigned to the out-of-band Ethernet management ports.
Parameters	<i>ip-prefix\ip-prefix-length</i> — The IP address in dotted decimal notation.
Values	ipv4-prefix a.b.c.d (host bits must be 0) ipv6-prefix - x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D
Values	ipv4-prefix-length 0 — 32
Values	ipv6-prefix-length 0 — 128

eth-mgmt-autoneg

Note: This command is not supported on 7210 SAS-D devices.

Syntax	[no] eth-mgmt-autoneg
Context	bof
Description	This command enables speed and duplex Auto-negotiation on the management Ethernet port in the running configuration and the Boot Option File (BOF). The no form of the command disables the Auto-negotiate feature on this port.
Default	eth-mgmt-autoneg — Auto-negotiation is enabled on the management Ethernet port.

eth-mgmt-disabled

Note: This command is not supported on 7210 SAS-D devices.

Syntax	[no] eth-mgmt-disabled
Context	bof
Description	This command allows the user to enable or disable the out-of-band management Ethernet port for use during boot up. The no form of the command enables the port.
Default	eth-mgmt-disabled

eth-mgmt-duplex

Note: This command is not supported on 7210 SAS-D devices.

Syntax	eth-mgmt-duplex {full half}
Context	bof
Description	This command configures the duplex mode of the management Ethernet port when Auto-negotiation is disabled in the running configuration and the Boot Option File (BOF). This configuration command allows for the configuration of the duplex mode of the Ethernet port. If the port is configured to Auto-negotiate, this parameter will be ignored.
Default	eth-mgmt-duplex full — Full duplex operation.
Parameters	<i>full</i> — Sets the link to full duplex mode. <i>half</i> — Sets the link to half duplex mode.

eth-mgmt-route

Note: This command is not supported on 7210 SAS-D devices.

Syntax	[no] eth-mgmt-route ip-prefix/ip-prefix-length next-hop ip-address
Context	bof
Description	This command creates a static route entry for the 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 Ethernet port. To reduce configuration, manual address aggregation should be applied where possible. A static default (0.0.0.0 or 0) route cannot be configured on the management Ethernet port. A maximum of ten static routes can be configured on the management Ethernet port. The no form of the command deletes the static route.
Default	No default routes are configured.
Parameters	<i>ip-prefix\ip-prefix-length</i> — The destination address of the static route in dotted decimal notation.

	<i>100</i> — The destination address of the static route in dotted decimal notation.
Values	ip-prefix ip-prefix-length: ipv4-prefix a.b.c.d (host bits must be zero) ipv4-prefix-length 0 — 32 ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D
Values	Values mask — The subnet mask, expressed as an integer or in dotted decimal notation. 0 — 32 (mask length), 128.0.0.0 — 255.255.255.255 (dotted decimal) ipv6-prefix-length - 0 — 128
next-hop	<i>ip-address</i> — The next hop IP address used to reach the destination.
Values	ipv4-address - a.b.c.d ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D
	The destination address of the static route in dotted decimal notation.

eth-mgmt-speed

Note: This command is not supported on 7210 SAS-D devices.

Syntax	speed <i>speed</i>
Context	bof
Description	This command configures the speed for the management Ethernet port when Auto-negotiation is disabled in the running configuration and the Boot Option File (BOF). If the port is configured to Auto-negotiate, this parameter is ignored.
Default	speed 100 — 100 M/bps operation.
Parameters	<i>10</i> — Sets the link to 10 M/bps speed. <i>100</i> — Sets the link to 100 M/bps speed.

DNS Configuration Commands

dns-domain

Syntax	dns-domain <i>dns-name</i> no dns-domain
Context	bof
Description	This command configures the domain name used when performing DNS address resolution. This is a required parameter if DNS address resolution is required. Only a single domain name can be configured. If multiple domain statements are configured, the last one encountered is used. The no form of the command removes the domain name from the configuration.
Default	no dns-domain — No DNS domain name is configured.
Parameters	<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	This command configures the primary DNS server used for DNS name resolution. DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files. The no form of the command removes the primary DNS server from the configuration.
Default	no primary-dns — No primary DNS server is configured.
Parameters	<i>ip-address</i> — The IP address of the primary DNS server. Values ipv4-address - a.b.c.d ipv6-address - x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D

secondary-dns

[no] secondary-dns *ip-address*

Context bof

Description This command configures the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the secondary DNS server from the configuration.

Default **no secondary-dns** — No secondary DNS server is configured.

Parameters *ip-address* — The IP address of the secondary DNS server.

Values

- ipv4-address - a.b.c.d
- ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
 x:x:x:x:x:x:d.d.d.d
 x - [0..FFFF]H
 d - [0..255]D

tertiary-dns

Syntax **tertiary-dns** *ip-address*
no tertiary-dns

Context bof

Description This command configures the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the tertiary DNS server from the configuration.

Default **no tertiary-dns** — No tertiary DNS server is configured.

Parameters *ip-address* — The IP address of the tertiary DNS server.

Values

- ipv4-address - a.b.c.d
- ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
 x:x:x:x:x:x:d.d.d.d
 x - [0..FFFF]H
 d - [0..255]D

Show Commands

bof

Syntax	bof [<i>cflash-id</i> 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	<i>cflash-id</i>. The cflash directory name. Values <i>cf1</i>: <i>booted</i> — Displays the boot option file used to boot the system.
Output	Show BOF Fields — The following table describes BOF output fields.

Table 15: Show BOF Output Fields

Label	Description
<i>primary-image</i>	The primary location of the directory that contains the runtime images of both CPM and IOM.
<i>primary-config</i>	The primary location of the file that contains the configuration.
<i>primary-dns</i>	The primary DNS server for resolution of host names to IP addresses.
<i>secondary-image</i>	The secondary location of the directory that contains the runtime images of both CPM and IOM.
<i>secondary-config</i>	The secondary location of the file that contains the configuration.
<i>secondary-dns</i>	The secondary DNS server for resolution of host names to IP addresses.
<i>tertiary-image</i>	The tertiary location of the directory that contains the runtime images of both CPM and IOM.
<i>tertiary-config</i>	The tertiary location of the file that contains the configuration.
<i>tertiary-dns</i>	The tertiary DNS server for resolution of host names to IP addresses.
<i>persist</i>	<i>on</i> — Persistent indexes between system reboots is enabled. <i>off</i> — Persistent indexes between system reboots is disabled.
<i>wait</i>	The time configured for the boot to pause while waiting for console input.

Table 15: Show BOF Output Fields (Continued)

Label	Description
autonegotiate	No autonegotiate — Autonegotiate not enabled. autonegotiate — Autonegotiate is enabled.
console speed	The console port baud rate.
ping-address	The IPv4 IP address to be used for ping-test after auto-init.
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.
console-disabled	Displays the status of serial port console.

Table 16: Show BOF Output Fields (supported only on 7210 SAS-E)

Label	Description
eth-mgmt-disabled	Displays if Ethernet management is disabled.
eth-mgmt-addressg	Displays the Ethernet management address.
eth-mgmt-route	Displays the Ethernet Management route.
eth-mgmt-autoneg	Displays if the auto-negotiate is enabled.
eth-mgmt-duplex	Displays the mode of the Ethernet management port.
eth-mgmt-speed	Displays the Ethernet management speed.

Sample Output

```
*A:ALA# show bof cfl:
```

```
=====
```

```
BOF on cfl:
```

```
=====
```



```

primary-image      ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
secondary-image    ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
tertiary-image     ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
primary-dns        135.254.244.204
dns-domain         in.lucent.com
ping 10.135.16.90
#uplinkA Port Settings:
uplinkA-port       1/1/1
uplinkA-address    192.168.1.11/24
uplinkA-vlan       0
uplinkA-route      10.135.0.0/16 next-hop 192.168.1.1
#uplinkB Port Settings:
uplinkB-port       1/1/2
uplinkB-address    0
uplinkB-vlan       0
#System Settings:
wait               3
persist            on
console-speed      115200
no console-disabled

=====
*A:ALA#
*A:ALA# show bof booted
=====
System booted with BOF
=====
primary-image      ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
secondary-image    ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
tertiary-image     ftp://*:~@10.135.16.90/./images/auto-boot/solution/bothx.tim
primary-dns        135.254.244.204
dns-domain         in.lucent.com
ping-address       10.135.16.90
#uplinkA Port Settings:
uplinkA-port       1/1/1
uplinkA-address    192.168.1.11/24
uplinkA-vlan       0
uplinkA-route      10.135.0.0/16 next-hop 192.168.1.1
#uplinkB Port Settings:
uplinkB-port       1/1/2
uplinkB-address    0
uplinkB-vlan       0
#System Settings:
wait               3
persist            on
console-speed      115200
no console-disabled

=====
*A:ALA#

```

boot-messages

Syntax	boot-messages
Context	show
Description	This command displays boot messages generated during the last system boot.
Output	Show Boot Messages Fields — The following output shows boot message output fields.

Sample Output

```
=====
cf1:/bootlog.txt
=====
Bootlog started for Version V-0.0.I317
Build V-0.0.I317 bootrom/mpc 7xxx
Built on Tue Jan 6 02:23:14 IST 2009 by panosbld in /panosbld/ws/panos/main

?Attempting to load from file cf1:/boot.tim
Version L-0.0.I312, Fri Jan 2 04:26:32 IST 2009 by panosbld in /panosbld/ws/panos/
main
text:(3002475-->12623392) + data:(550940-->2414128)
Starting at 0xb000000...

Total Memory: 512MB Chassis Type: sas Card Type: badami_7210
TiMOS-L-0.0.I312 boot/mpc ALCATEL SAS-E 7210 Copyright (c) 2000-2009 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Fri Jan 2 04:26:32 IST 2009 by panosbld in /panosbld/ws/panos/main

TiMOS BOOT LOADER
Extended checks enabled with overhead of 36B
Time from clock is THU JAN 08 16:04:05 2009 UTC
Switching serial output to sync mode... done

Looking for cf1:/bof.cfg ... OK, reading

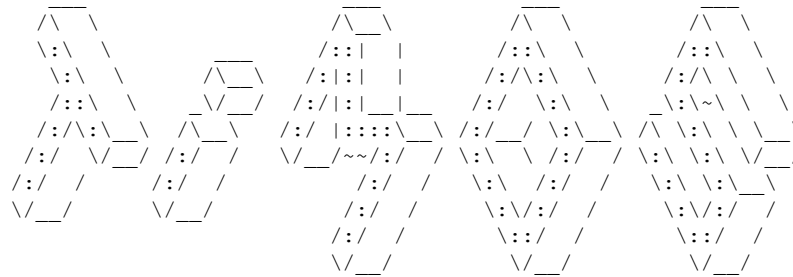
Contents of Boot Options File on cf1:
    primary-image      ftp://*:192.168.170.22/import/panos_nightly_builds/1.0/B1-
12/STU-sultan/both.tim
    primary-config      cf1:\config.cfg
#uplinkA Port Settings:
    uplinkA-port        1/1/13
    uplinkA-address     10.135.17.246/24
    uplinkA-vlan         null
    uplinkA-route       10.135.0.0/16 next-hop 10.135.17.1
    uplinkA-route       192.168.0.0/16 next-hop 10.135.17.1
#uplinkB Port Settings:
    uplinkB-port        1/1/2
    uplinkB-address     0
    uplinkB-vlan         0
#System Settings:
    wait                3
    persist              off
    console-speed       115200

Hit a key within 1 second to change boot parms...
```

```
Configuring Network with uplinkA Port Setting.....
Primary config file present at: cfl:\config.cfg

Primary image location: ftp://*:~@192.168.170.22/import/panos_nightly_builds/1.0/B1-12/STU-sultan/both.tim
Initializing uplinkA port using IP addr 10.135.17.246.
Loading image ftp://*:~@192.168.170.22/import/panos_nightly_builds/1.0/B1-12/STU-sultan/both.tim
Version B-1.0.B1-12, Wed Jan 7 00:58:35 IST 2009 by builder in /builder/ws/panos/main
text:(27022791-->84574868) + data:(1921023-->10720420)
Executing TiMOS image at 0x100000
```

```
Total Memory: 512MB Chassis Type: sas Card Type: badami_7210
TiMOS-B-1.0.B1-12 both/mpc ALCATEL 7210 Copyright (c) 2000-2009 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jan 7 00:58:35 IST 2009 by builder in /builder/ws/panos/main
```



Time from clock is THU JAN 08 16:05:20 2009 UTC

```
Attempting to exec primary configuration file:
'cfl:\config.cfg' ...
System Configuration
System Security Configuration
Log Configuration
System Security Cpm Hw Filters Configuration
QoS Slope and Queue Policies Configuration
Port Scheduler Policies Configuration
Card Configuration
Port Configuration
Management Router Configuration
Router (Network Side) Configuration
Static Route Configuration
Service Configuration
Router (Service Side) Configuration
Executed 234 lines in 0.1 seconds from file cfl:\config.cfg
```

```
INFO: CLI #1008 The SNMP daemon is disabled. To enable SNMP, execute the command
'config>system>snmp no shutdown'.
TiMOS-B-1.0.B1-12 both/mpc ALCATEL SAS-E 7210 Copyright (c) 2000-2008 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jan 7 00:58:35 IST 2009 by builder in /builder/ws/panos/main
```

Login:

System Management

In This Chapter

This chapter provides information about configuring basic system management parameters.

Topics in this chapter include:

- [System Management Parameters on page 174](#)
 - [System Information on page 174](#)
 - [System Name on page 174](#)
 - [System Contact on page 174](#)
 - [System Location on page 175](#)
 - [System Coordinates on page 175](#)
 - [Naming Objects on page 175](#)
 - [Naming Objects on page 175](#)
 - [System Time on page 177](#)
 - [Time Zones on page 177](#)
 - [Network Time Protocol \(NTP\) on page 179](#)
 - [SNTP Time Synchronization on page 180](#)
 - [CRON on page 181](#)
- [High Availability on page 182](#)
 - [HA Features on page 182](#)
 - [HA Features on page 182](#)
 - [Redundancy on page 182](#)

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 CLI code as well as time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) properties, CRON and synchronization properties.

System Information

System information components include:

- [System Name on page 174](#)
 - [System Contact on page 174](#)
 - [System Location on page 175](#)
 - [System Coordinates on page 175](#)
 - [Naming Objects on page 175](#)
-

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.

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.

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.

System Coordinates

The system coordinates is the Alcatel-Lucent 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.

Naming Objects

It is discouraged to configure named objects with a name that starts with “_tmnx_” and with “_” in general.

Common Language Location Identifier

A Common Language Location Identifier (CLLI) code string for the device is an 11-character standardized geographic identifier that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry. The CLLI code is stored in the Alcatel-Lucent Chassis MIB `tmnxChassisCLLIcode` object.

The CLLI code can be any ASCII printable text string of up to 11 characters.

System Time

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 software has options for local time translation as well as system clock synchronization.

System time parameters include:

- [Time Zones on page 177](#)
- [Network Time Protocol \(NTP\) on page 179](#)
- [SNTP Time Synchronization on page 180](#)
- [CRON on page 181](#)

Time Zones

Setting a time zone in allows for times to be displayed in the local time rather than in UTC. The 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 system-defined time zones are listed in [Table 17](#) which includes both time zones with and without summer time correction.

Table 17: System-defined Time Zones

Acronym	Time Zone Name	UTC Offset
Europe:		
GMT	Greenwich Mean Time	UTC
BST	British Summer Time	UTC +1
IST	Irish Summer Time	UTC +1*
WET	Western Europe Time	UTC
WEST	Western Europe Summer Time	UTC +1
CET	Central Europe Time	UTC +1
CEST	Central Europe Summer Time	UTC +2
EET	Eastern Europe Time	UTC +2
EEST	Eastern Europe Summer Time	UTC +3

Table 17: System-defined Time Zones (Continued)

Acronym	Time Zone Name	UTC Offset
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
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

Network Time Protocol (NTP)

NTP is the Network Time Protocol defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*. 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 7210 SAS E device cannot act as stratum-1 servers but can act as stratum-2 devices as a network connection to an NTP server is required.

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.

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.
- Broadcast modes — When operating in this mode, the node will receive or send using a broadcast address.
- 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.
-

SNTP Time Synchronization

For synchronizing the system clock with outside time sources, the 7210 SAS OS software 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.

In the 7210 SAS OS software, the SNTP client can be configured for either broadcast or unicast client mode.

CRON

The CRON feature supports the Service Assurance Agent (SAA) functions as well as the ability to schedule turning on and off policies to meet “Time of Day” requirements. CRON functionality includes the ability to specify the commands that need to be run, when they will be scheduled, including one-time only functionality (oneshot), interval and calendar functions, as well as where to store the output of the results. In addition, CRON can specify the relationship between input, output and schedule. 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 features are saved to the configuration file.

CRON features run serially with at least 255 separate schedules and scripts. Each instance can support a schedule where the event is executed any number of times.

The following CRON elements are supported:

- **Action** — Parameters for a script including the maximum amount of time to keep the results from a script run, the maximum amount of time a script may run, the maximum number of script runs to store and the location to store the results.
- **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).
- **Script** — The script command opens a new nodal context which contains information on a script.
- **Time Range** — ACLs and QoS policy configurations may be enhanced to support time based matching. CRON configuration includes time matching with the 'schedule' sub-command. Schedules are based on events; time-range defines an end-time used as a match criteria.
- **Time of Day** — Time of Day (TOD) suites are useful when configuring many types of time-based policies or when a large number of SAPs require the same type of TOD changes. The TOD suite may be configured while using specific ingress or egress ACLs or QoS policies, and is an enhancement of the ingress and egress CLI trees.

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.

HA Features

As more and more critical commercial applications move onto the IP networks, providing high availability services becomes increasingly important. This section describes high availability features for devices.

- [Redundancy on page 182](#)
→ [Component Redundancy on page 183](#)
-

Redundancy

The redundancy features enable the duplication of data elements to maintain service continuation in case of outages or component failure.

Component Redundancy

7210 SAS-Series component redundancy is critical to reduce MTTR for the system and primarily consists of the following features for 7210 SAS-E devices:

- Redundant power supply — A power module can be removed without impact on traffic.
- Fan module — The fan module contains three fans. Failure of one or more fans does not impact traffic.
- Hot swap — The power supply and fan module supports hot swapping.

For 7210 SAS-D devices:

- 7210 SAS-D has an integrated AC or DC power supply. Redundant external backup power supply is available only on 7210 SAS-D ETR variant. Use of redundant external backup power supply is optional.
- Fan module — 7210 SAS-D 128 MB devices support passive cooling. It has a fan to allow air circulation (and not cooling). By default the fan mode is set to 'auto'. In "auto" mode, by default, the software determines when to turn the fan 'on' and when to switch it 'off'. This can be changed by the operator using the CLI command "configure> system> fan". Operators have an option to switch off the fan permanently or turn it on permanently.
- Hot swap — Power supply integrated into chassis. Hot swapping is not supported. The external power supply backup connection can be added or removed anytime on 7210 SAS-D ETR.

Temperature Threshold Alarm and Fan Speed

In the 7210 SAS E device, if the chassis temperature crosses a threshold of 58 degrees centigrade , the system raises an software alarm for over-temperature. When the temperature reduces below 58C, the over-temperature alarm is cleared by the system.

The fan operates at two speeds- half speed and full speed. When the temperature of the chassis raises above 42 degrees centigrade the fan speed changes to full speed and when the temperature reduces to 37 degrees centigrade, the fan speed changes to half speed.

The 7210 SAS-D devices do not support any alarm contact outputs, hence when the system raises an alarm it is only logged. The system status LED is used to indicate an alarm in applicable cases. Listed below in table X are the temperature thresholds for 7210 SAS-D devices:

Table 18: Temperature Thresholds for 7210 SAS-D Devices

Device Variants	Min. Temperature (in degree centigrade)	Max. Temperature (in degree centigrade)
7210 SAS-D	0	45
7210 SAS-D ETR	-30	60

The temperature threshold is measured by the sensors inside the chassis and is typically more than the aisle ambient temperature. The threshold temperature is not user configurable.

Over-temperature is alarm raised when the temperature of the device exceeds 45 in degree centigrade in 7210 SAS-D 6T4F and 60 in degree centigrade in 7210 SAS-D 6T4F ETR variant.

Note: 7210 SAS-D devices do not use fans for cooling. The device uses natural air flows for cooling. 7210 SAS-D 128MB devices has a fan to provide air circulation.

Synchronization

The 7210 SAS-D implements distribution of timing information through line timing mode.

Note: 7210 SAS-E does not implement any synchronization mechanisms.

Line Timing Mode

Line timing from Synchronous Ethernet port provides the best synchronization performance through a synchronization distribution network. Line timing mode derives the timing information from the Ethernet ports. This mode is immune to any Packet Delay Variation (PDV) occurring on Layer 2 or Layer 3 links. Line timing is supported on the Ethernet SFP ports with SFPs that support Synchronous Ethernet (supported only with 1Gbps speed). The fixed copper ports support synchronous ethernet. The fixed copper ports on 7210 SAS-D, can be used as obtain a syncE reference (port-clock mode must be slave) or to distribute syncE to other nodes (port-clock mode must be master). Please see the CLI command `config> port> ethernet> port-clock` in the 7210 SAS-DE Interfaces User Guide. Note that auto-negotiation (or auto-negotiation limited) must be turned on and speed must be 1Gbps, before using syncE on the fixed copper ports.

Synchronous Ethernet

Synchronous Ethernet is a variant of line timing supported on the on Ethernet SFP ports with SFPs that support Synchronous Ethernet. When synchronous Ethernet is enabled, the operator can select an Ethernet port as a candidate for timing reference. The timing recovered from this port is used to time the system. This ensures all the system outputs are locked to a stable and traceable frequency source.

Synchronous Ethernet is active at Layer 1 and monitors the precision of the following:

- Timing of signal transitions to be relayed.
- Recovery of accurate frequencies.

Synchronous Ethernet is not impacted by traffic load and therefore not affected by packet loss or PDV that occurs with timing methods that use higher layers of the networking technology.

Synchronous Ethernet can be used only for end-to-end network synchronization when all intermediate switching nodes in the network have hardware and software support for Synchronous Ethernet.

Network Synchronization

This section describes network synchronization capabilities available on 7210 SAS-D platform. In 7210 SAS-D devices network synchronization is achieved through line timing from synchronous Ethernet ports.

Network synchronization is commonly distributed in a hierarchical master-slave topology at the physical layer as shown in [Figure 12](#).

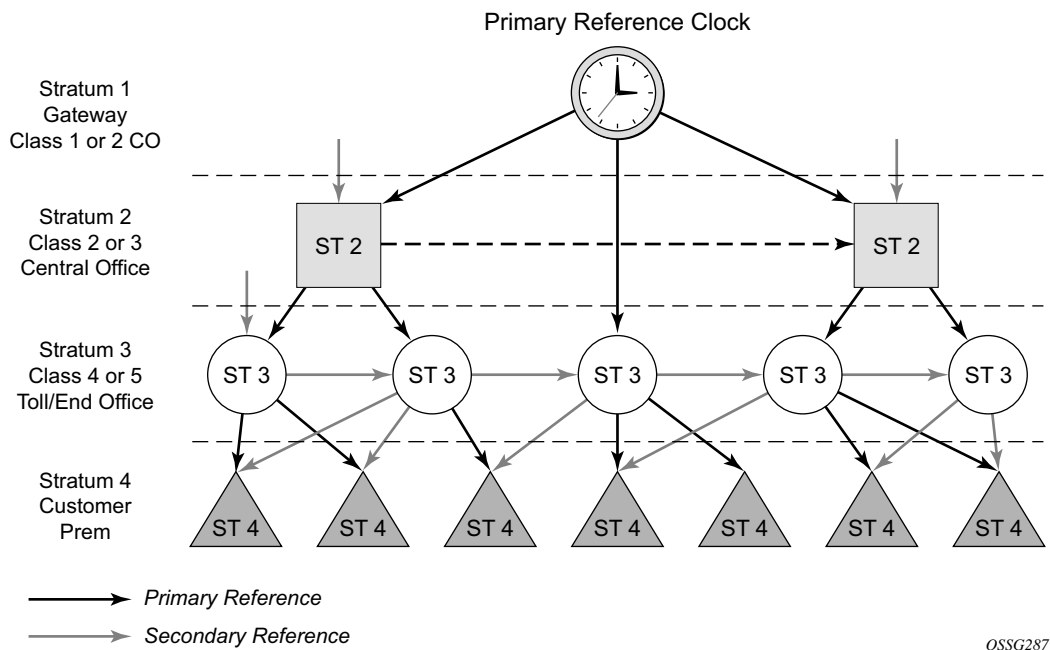


Figure 12: Conventional Network Timing Architecture (North American Nomenclature)

The architecture shown in [Figure 12](#) 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 does not 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 timeframe. 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.

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.

Central Synchronization Sub-System

The timing subsystem for the 7210 SAS 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.

To train the local oscillator, the system has the option to select from two timing inputs. The priority order of these references must be specified. This is a simple ordered list of inputs: {ref1, ref2}. The CPM clock output shall have the ability to drive the clocking for all line cards in the system. The 7210 SAS supports selection of the node reference using Quality Level (QL) indications. See [Figure 13](#) for a description of synchronization reference selection.

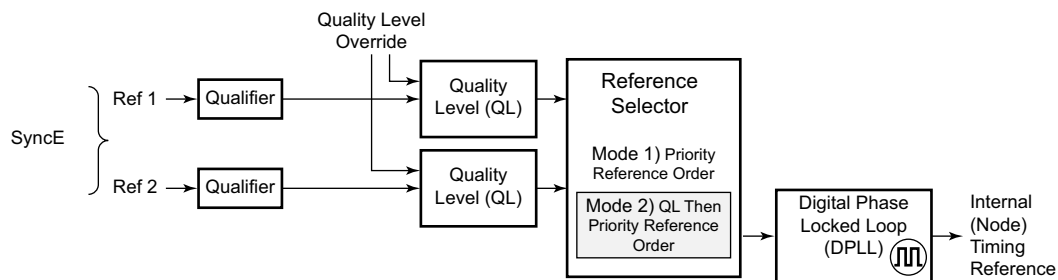


Figure 13: Synchronization Reference Selection

The recovered clock derives its timing from synchronous Ethernet ports. If QL selection mode is disabled, the reversion setting specifies as to when the central clock can re-select a previously failed reference.

The [Table 19](#) shows the selection followed for two references in both revertive and non-revertive modes:

Table 19: 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

Synchronization Status Messages (SSM)

Note: Synchronous status messages are supported only on 7210 SAS-D devices.

SSM provides a mechanism to allow the synchronization distribution network to determine both the quality level of the clock sourcing a given synchronisation 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.

IEEE 1588v2 PTP

Note: This feature is applicable only to the 7210 SAS-D ETR device.

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard 1588 PTP 2008.

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 source over a network that may or may not be PTP-aware. PTP has several advantages over ACR. It is a standards-based protocol, has lower bandwidth requirements, can transport both frequency and time, and can potentially provide better performance.

There are five basic types of PTP devices, as listed below:

- Ordinary clock
- Boundary clock
- End-to-end transparent clock
- Peer-to-peer transparent clock
- Management node

The 7210 SAS supports the ordinary clock in slave mode or the boundary clock. The boundary clock and ordinary clock slave can be used for both frequency and time distribution. 7210 SAS does not support ordinary clock in master mode.

The 7210 SAS communicates with peer IEEE 1588v2 clocks; see [Figure 14](#). These peers can be ordinary clock slaves or boundary clocks. Each peer is identified by the IPv4 address to be used for communications between the two clocks. There are two types of peers: configured and discovered. The 7210 SAS operating as an ordinary clock slave or as a boundary clock should have configured peers for each PTP neighbor clock from which it might accept synchronization information. The 7210 SAS initiates unicast sessions with all configured peers. A 7210 SAS operating as an 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. The 7210 SAS can deliver synchronization information toward discovered peers (that is, slaves).

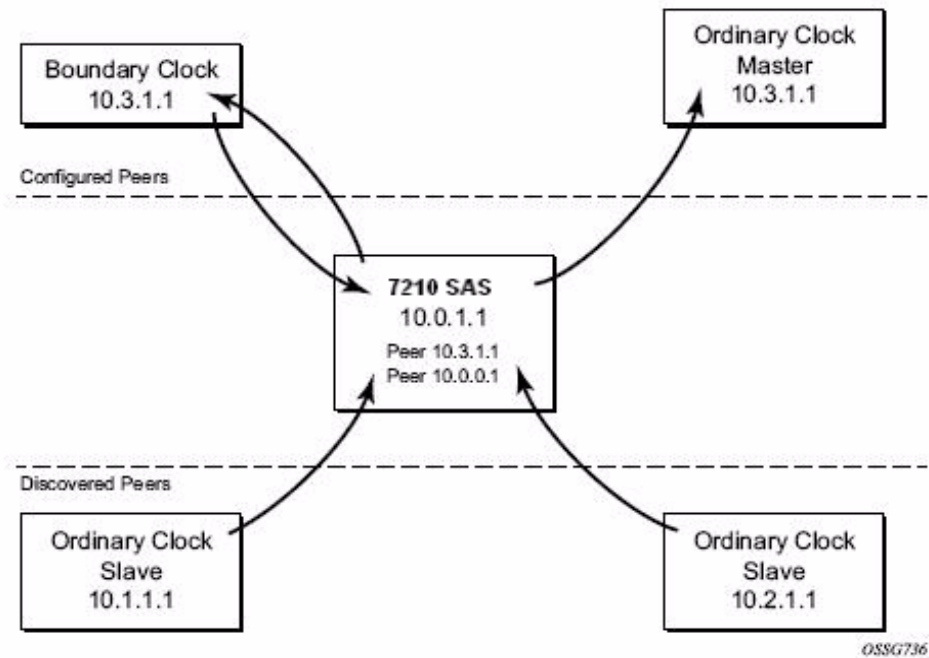


Figure 14: Peer Clocks

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.

7210 SAS currently supports two profiles:

- IEEE 1588v2 default profile
- ITU-T Telecom profile (G.8265.1)

In both cases, communications between clocks utilize the Unicast communication procedures of the IEEE standard. The transport layer uses UDP/IPv4 encapsulation.

When a 7210 SAS receives Announce messages from one or more configured peers, 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 7210 SAS sets its local parameters as follows:

Table 20: 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 – router configured as ordinary clock master and is locked to an external reference 14 – router configured as ordinary clock master and in holdover after having been locked to an external source 248 – router configured as ordinary clock master and is in free run or the router is configured as a boundary clock 255 – router configured as ordinary clock slave
clockAccuracy	FE - Unknown
offsetScaledLogVariance	FFFF – not computed

If the profile setting for the clock is itu-telecom-freq (ITU G.8265.1 profile), the precedence order for the best master selection algorithm is:

- clock class
- priority

The 7210 SAS sets its local parameters as follows:

Table 21: 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 of the 7210 SR as per Table 1/ G.8265.1 255 – the 7210 SAS is configured as ordinary clock slave

The ITU-T profile is for use in an environment with only ordinary clock masters and slaves for frequency distribution. The default profile should be used for all other cases.

The 7210 SAS can support a limited amount of configured peers (possible Master or neighbor boundary clocks) and a limited amount of discovered peers (slaves). These peers use the Unicast Negotiation procedures to request service from the 7210 SAS clock. A neighbor boundary clock counts for two peers (both a configured and a discovered peer) toward the maximum limit.

[Figure 15](#) 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.

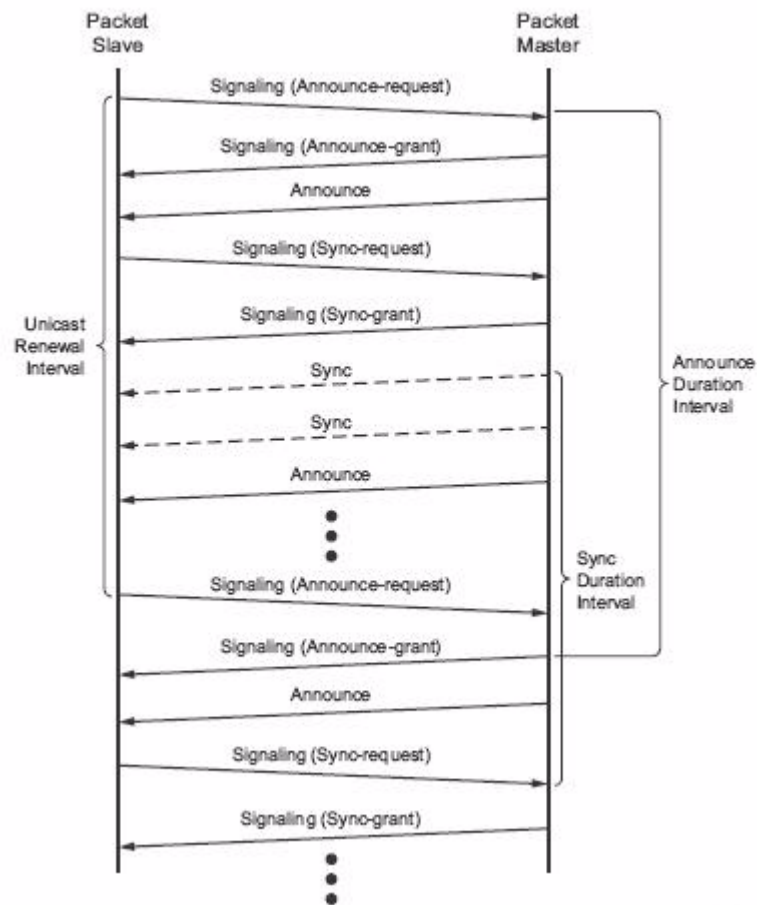


Figure 15: Messaging Sequence Between the PTP Slave Clock and PTP Master Clocks

PTP Clock Synchronization

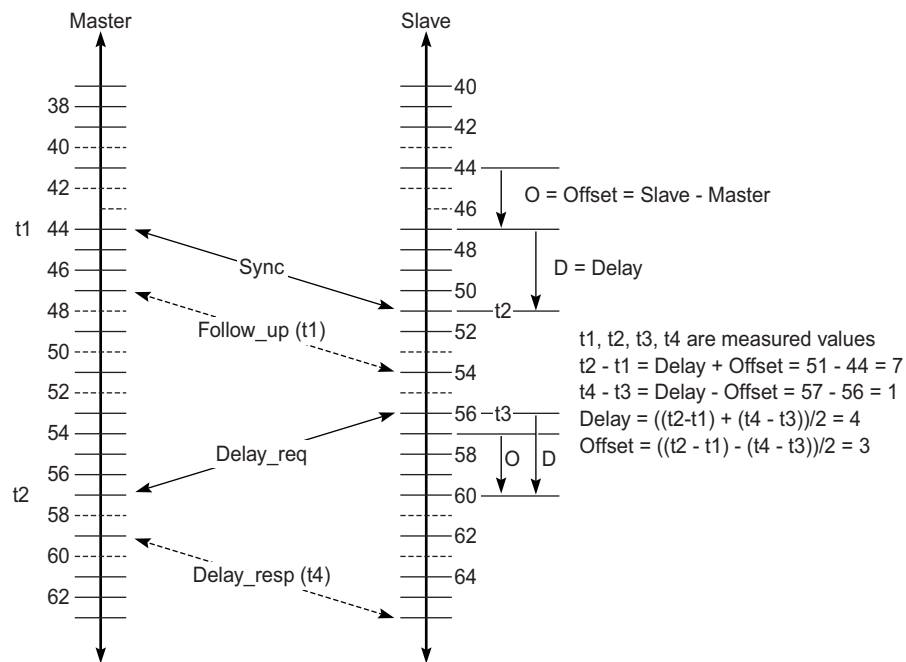
The IEEE 1588v2 standard synchronizes the frequency and time from a master clock to one or more slave clocks over a packet stream. This packet-based synchronization can be over UDP/IP or Ethernet and can be multicast or unicast. Only IPv4 unicast mode with unicast negotiation is supported.

As part of the basic synchronization timing computation, a number of event messages are defined for synchronization messaging between the PTP slave clock and PTP master clock. A one-step or

two-step synchronization operation can be used, with the two-step operation requiring a follow-up message after each synchronization message. Only two-step operation is supported on the 7210 SAS devices.

During startup, the PTP slave clock receives the synchronization messages from the PTP master clock before a network delay calculation is made. Prior to any delay calculation, the delay is assumed to be zero. A drift compensation is activated after a number of synchronization message intervals occur. The expected interval between the reception of synchronization messages is user-configurable.

The basic synchronization timing computation between the PTP slave clock and PTP best master is illustrated in Figure 16. This figure illustrates the offset of the slave clock referenced to the best master signal during startup.



OSSG644

Figure 16: PTP Slave Clock and Master Clock Synchronization Timing Computation

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 7210 SAS uses the four timestamps exchanged using the IEEE 1588v2 messages to determine the offset between the 7210 SAS time base and the external master clock time base. The 7210 SAS determines the offset adjustment and then in between these adjustments, it maintains the progression of time using the frequency from the central clock of the node. This allows time to be maintained using 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 the PTP input reference enabled.

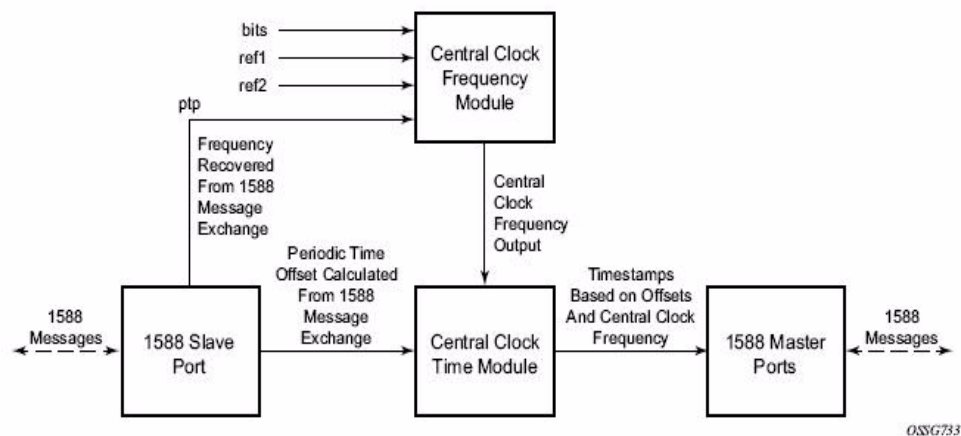


Figure 17: Using IEEE 1588v2 For Time Distribution

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. 7210 SAS that are 1588v2 capable supports port-based time stamping.

PTP Capabilities

PTP messages are supported via IPv4 unicast with a fixed IP header size. [Table 22](#) describes the support message rates for slave and master states. The ordinary clock can be used in only slave mode. The boundary clock can be in both of these states.

Table 22: Support Message Rates for Slave and Master Clock States

Support Message	Slave Clock	Master Clock	
	Request Rate	Grant Rate	
		Min	Max
Announce	1 packet every 2 seconds	1 packet every 2 seconds	1 packet every 2 seconds
Sync	Default is 64 packets/second. Provides anoption to configure lesser rates.	8 packets/seconds	128 packets/seconds
Delay_Resp	Default is 64 packets/second. Provides anoption to configure lesser rates.	8 packets/seconds	128 packets/seconds
(Duration)	300 seconds	1 second	1000 seconds

State and statistics data for each master clock are available to assist in the detection of failures or unusual situations.

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 7210 SAS 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 18 shows a PTP ordinary slave clock network configuration.

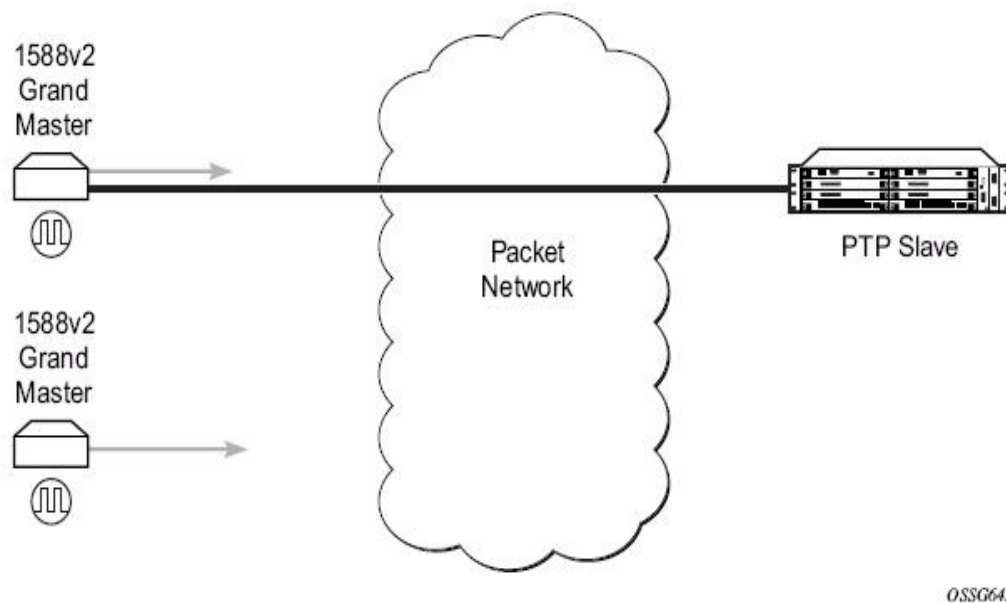


Figure 18: Slave Clock

The PTP slave capability is implemented on all the Ethernet port available on the 7210 SAS-M

Figure 18 shows the operation of an ordinary PTP clock in slave mode.

PTP Boundary Clock for Frequency and Time

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; see [Figure](#) . 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. The time scale recovered in the slave side of the boundary clock is used by the master side of the boundary clock. This allows time to be distributed across the boundary clock.

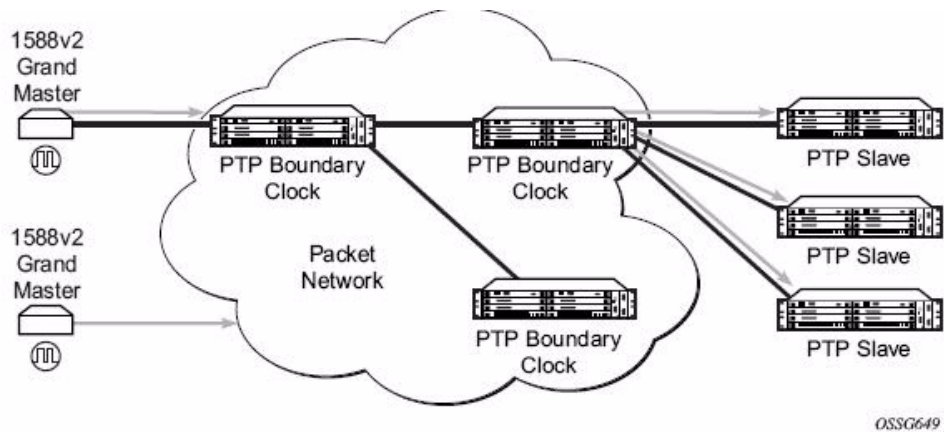


Figure 19: Boundary Clock

Configuration guidelines for PTP on 7210 SAS-DETR

- Use of PTP and syncE as a reference simultaneously is not allowed. User can configure either syncE as a reference or PTP as a reference, but not both together.
- 7210 SAS-D ETR node uses CPU processing cycles for frequency and time recovery. It is highly recommended to use PTP only in hybrid mode (that is, SyncE for frequency recovery and PTP for time recovery). Hybrid mode allows the node to recover very stable frequency using SyncE and recovers time using reduced PTP packet rate. It reduces the CPU processing cycles needed, helping customers to scale better.

Configuration to change reference from syncE to PTP

The following are the configuration steps to change reference from SyncE to PTP.

1. Initially for Standalone PTP :

```
configure >system >ptp >no shutdown

config> system> sync-if-timing> begin
    ptp
    no shutdown
    exit
    ref-order ptp [Must be configured]

config> system> sync-if-timing> commit
```

Note : Now the Frequency and Time is provide by PTP only.

2. To changeover to use syncE the following must be executed:

```
config> system> sync-if-timing> begin
    ptp
    shutdown
    exit

config> system> sync-if-timing> commit

config> system> sync-if-timing> begin
    refl
    source-port 1/1/10
    no shutdown
    exit

    ref2
    source-port 1/1/11
    no shutdown
    exit

    ref-order refl ref2 -----> Or, the ref-order you want [But Must be configured]

    revert -----> If you want ref-order you have setup to take effect

    ql-selection -----> Optional , if we need Quality to be consisdered .

config> system> sync-if-timing> commit
```

Note : Now the frequency is provided by SyncE and TOD is provided by PTP [configure >system >ptp >no shutdown]. This is called Hybrid mode .

3. To change back to Stand alone PTP from SyncE, the following must be executed:

```
config> system> sync-if-timing> begin
    refl
        source-port 1/1/10 -----> Not Required if port is already con-
        figured, but in admin down state
        shutdown
    exit

    ref2
        source-port 1/1/11 -----> Not Required if port is already con-
        figured, but in admin down state
        shutdown
    exit

config> system> sync-if-timing> commit

config> system> sync-if-timing> begin
    ptp
        no shutdown
    exit

    ref-order ptp [Must be configured]

config> system> sync-if-timing> commit
```

Note : Now the Frequency and Time is provide by PTP [configure >system >ptp >no shutdown] only. This is a standalone PTP mode.

Management of 1830 VWM

Note: This feature is supported only on 7210 SAS-E.

7210 SAS supports use and management of the 1830 VWM flexible CWDM clip-on device. 1830 VWM is a cost-optimized managed CWDM passive device, which is add-on shelf/NE and provides CWDM extension to devices that do not have an in-built CWDM capabilities. 1830 VWM can act as an FOADM (Fixed Channel Optical Add-Drop Multiplexer) or multiplexer/demultiplexer unit. It allows operators to use the existing fiber (or use less fiber) and increase the bandwidth capacity available for carrying service traffic.

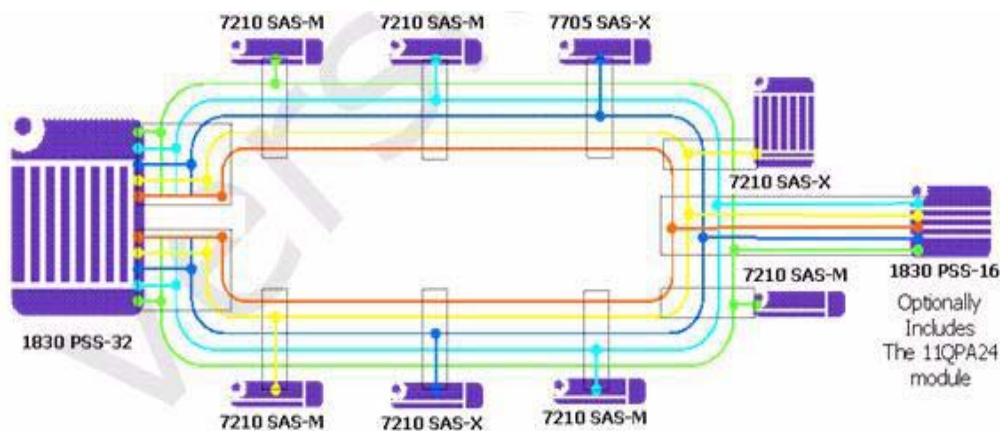
For more information about 1830 VWM, see “1830 VWM Product User Guides”.

To manage the device, user needs to plug-in the 1830 VWM shelf to the USB port on the 7210 SAS-E

Introduction to 1830 VWM CWDM Passive Optical device

1830 VWM CWDM Passive Optical device can be used in point-to-point or ring deployments to multiplex multiple CWDM channels over a single fiber. This functionality either reuses the existing fiber or uses a single fiber to meet the requirements for the always increasing demand for service bandwidth. Up to 8 fixed CWDM channels is multiplexed over a single fiber using this unit.

Figure 20: Optical Ring with 7210 SAS and 1830 VWM Passive Optical unit



In the above [Figure 20](#), there are 5 CWDM channels that are multiplexed over a single fiber. There are two types of ring locations. One is a channel termination location, with the 1830 PSS-32 that

optically terminates all the channels using either the 4-channel or the 8-channel termination module. These sites use the CWDM passive units to add or drop channel in both the directions (east and west), for traffic to be processed by the node. Additionally these sites provide express lanes for all the other channels (that is, those not processed locally by the node). The 1830 VWM provide an option for add or drop up to 1, 2, 4 channels of fixed wavelength to be processed locally by the node.

Feature Description

The 1830 VWM clip-on device can be connected to a master-shelf, i.e. the 7210 SAS node using the USB interface. Each of these clip-on devices is identified using the shelf ID set using the rotary dial provided on the device. To assist inventory management, the user must configure the vwm-shelf-id of the clip-on device attached to the USB interface using the CLI command `configure>system> vwm-shelf <id> create`. The vwm-shelf-id must match the shelf ID set using the rotary dial on the clip-on device. 7210 SAS devices, uses the configured vwm-shelf-id to communicate with the clip-on device. If these shelf IDs do not match, 7210 SAS cannot communicate to the device and will not provide any information about the device. 7210 SAS cannot detect a mismatch between the configured vwm-shelf-id and the shelf ID set on the rotary dial. It will raise an event or log to alert user about possible mismatch in configuration of shelf IDs. Only one 1830 VWM CWDM clip-on device can be connected to the USB interface of the 7210 SAS devices. Attempt to configure more than a single shelf-ID will result in an error. Users can use the show command provided by the 7210 SAS devices to display the shelf inventory information and alarm status information provided by the clip-on device.

NOTE: The users must ensure that they do not connect more than one device to the 7210 SAS devices.

7210 SAS also autodetects the device type when any of the supported devices are connected to the USB interface. Only approved USB mass storage device and optical clip-on devices can be plugged in to the USB port and are recognized as valid devices. All other unsupported devices will result in an error log being printed. A shelf created by the user will be operationally down when an unrecognized device plugged into the USB port. The user can interchange the device that's connected to the USB port without requiring a reboot. For example, in a production network, when the 7210 SAS is operating with a clip-on device; user can pull out the clip-on device, instead plug-in a USB mass-storage device to copy over image files or other files, and then plug back a clip-on device.

Configuration Guidelines

The shelf-ID on the rotary dial must be set to a digit between 1-7. Digits higher than 7 are not supported by 7210 SAS devices.

Link Layer Discovery Protocol (LLDP)

The IEEE 802.1ab Link Layer Discovery Protocol (LLDP) is a uni-directional protocol that uses the MAC layer to transmit specific information related to the capabilities and status of the local device. The LLDP can send as well as receive information from a remote device stored in the related MIB(s).

The LLDP does not contain a mechanism to solicit information received from other LLDP agents. The protocol also does not provide means to confirm the receipt of information. LLDP provides the flexibility of enabling a transmitter and receiver separately, therefore the following LLDP configurations are allowed:

- An LLDP agent can only transmit information.
- An LLDP agent can only receive information.
- An LLDP agent can transmit and receive information.

The information fields in each LLDP frame are contained in an LLDP Data Unit (LLDPDU) as a sequence of variable length information elements. Each information element includes Type, Length, and Value fields (TLVs).

- Type indicates the nature of information being transmitted.
- Length indicates the length of the information string in octets.
- Value is the actual information that is transmitted. (For example, a binary bit map or an alphanumeric string that can contain one or more fields).

Each LLDPDU contains four mandatory TLVs and optional TLVs selected by the Network Management. Below is the format of a LLDPDU:

- Chassis ID TLV
- Port ID TLV
- Time To Live TLV
- Zero or more optional TLVs, depending on the maximum size of the LLDPDU allowed.
- End Of LLDPDU TLV

An LLDP agent or port is identified by a concatenated string formed by the Chassis ID TLV and the Port ID TLV. This string is used by a recipient to identify an LLDP port or agent. The combination of the Port ID and Chassis ID TLVs remains unchanged until the port or agent is operational.

The TTL (Time To Live) field of an Time-To-Live TLV can be either zero or a non-zero value. A zero value in the TTL field notifies the receiving LLDP agent to immediately discard all information related to the sending LLDP agent. A non-zero value in the TTL field indicates the time duration for which the receiving LLDP agent should retain the sending LLDP agent's

information. The receiving LLDP agent discards all information related to the sending LLDP agent after the time interval indicated in the TTL field is complete.

Note: A TTL value of zero can be used to signal that the sending LLDP port has initiated a port shutdown procedure.

The End Of LLDPDU TLV indicates the end of the LLDPDU.

Listed below is the information included in the protocol defined by the IEEE 802.1ab standard:

- Connectivity and management information about the local station to adjacent stations on the same IEEE 802 LAN is advertised.
- Network management information from adjacent stations on the same IEEE 802 LAN is received.
- Operates with all IEEE 802 access protocols and network media.
- Network management information schema and object definitions that suitable for storing connection information about adjacent stations is established.
- Provides compatibility with a number of MIBs.

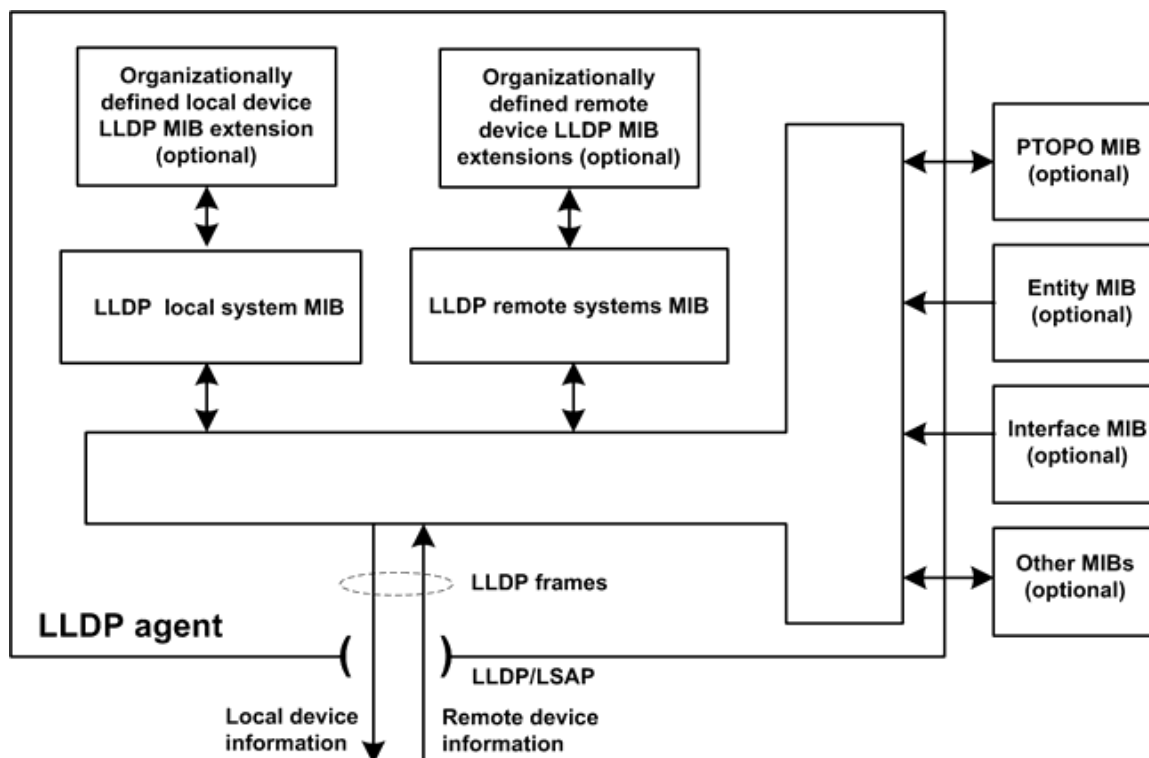


Figure 21: LLDP Internal Architecture for a Network Node

Link Layer Discovery Protocol (LLDP)

In order to detect and address network problems and inconsistencies in the configuration, the network operators can discover the topology information using LLDP. The Standard-based tools address the complex network scenarios where multiple devices from different vendors are interconnected using Ethernet interfaces.

The example displayed in [Figure 22](#) depicts a MPLS network that uses Ethernet interfaces in the core or as an access/handoff interfaces to connect to different kind of Ethernet enabled devices such as service gateway/routers, QinQ switches DSLAMs or customer equipment.

The topology information of the network in [Figure 22](#) can be discovered if, IEEE 802.1ab LLDP is running on each of the Ethernet interfaces in network.

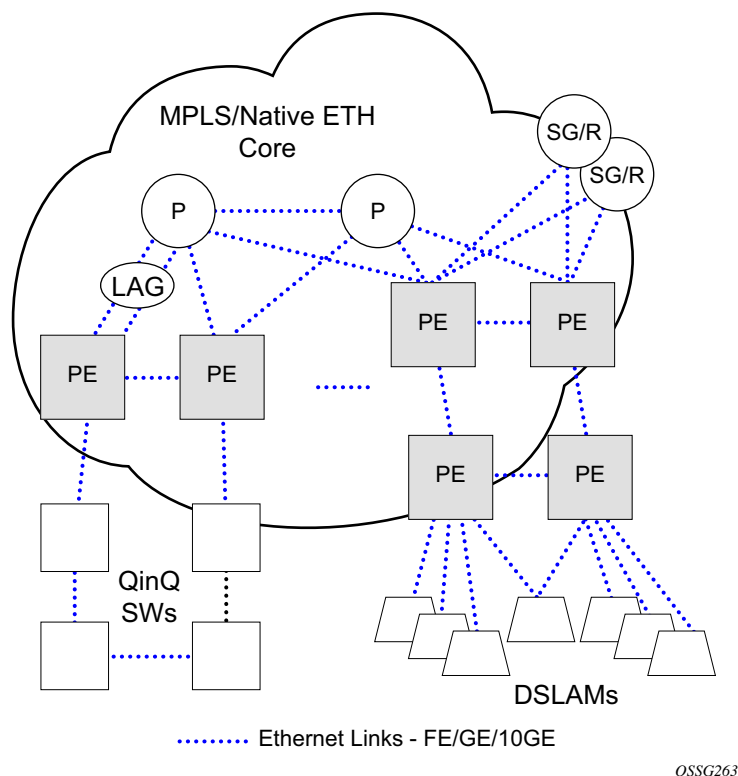


Figure 22: Customer Use Example For LLDP

System Configuration Process Overview

Figure 23 displays the process to provision basic system parameters.

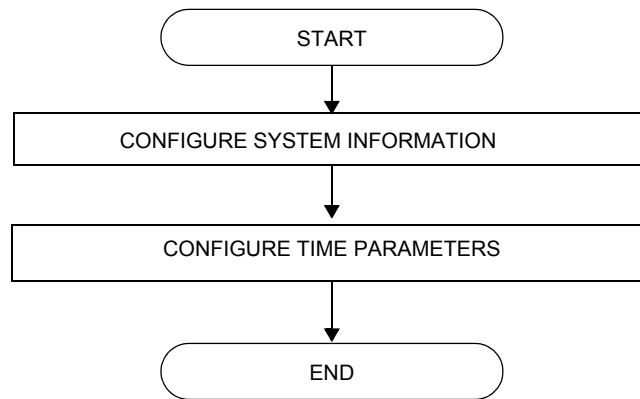


Figure 23: System Configuration and Implementation Flow

Configuration Notes

This section describes system configuration caveats.

General

- The 7210 SAS device must be properly initialized and the boot loader and BOF files successfully executed in order to access the CLI.

Configuring System Management with CLI

This section provides information about configuring system management features with CLI.

Topics in this chapter include:

- [Basic System Configuration on page 213](#)
- [Common Configuration Tasks on page 214](#)
- [System Information on page 215](#)
 - [System Information Parameters](#)
 - [Name on page 216](#)
 - [Contact on page 216](#)
 - [Location on page 217](#)
 - [CLLI Code on page 217](#)
 - [Coordinates on page 218](#)
 - [System Time Elements on page 219](#)
 - [Zone on page 219](#)
 - [Summer Time Conditions on page 221](#)
 - [NTP on page 222](#)
 - [SNTP on page 227](#)
 - [CRON on page 229](#)
- [System Administration Parameters on page 241](#)
 - [Validating the Golden Bootstrap Image on page 241](#)
 - [Updating the Golden Bootstrap Image on page 242](#)
 - [Disconnect on page 242](#)
 - [Set-time on page 243](#)
 - [Display-config on page 243](#)
 - [Tech-support on page 245](#)
 - [Save on page 245](#)
 - [Reboot on page 246](#)
 - [Post-Boot Configuration Extension Files on page 247](#)
- [Configuring System Monitoring Thresholds on page 253](#)

System Management

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 Option Files* section of this manual.

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.

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 on page 216](#)
- [System Time Elements on page 219](#)

The following example displays 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
          sntp
              shutdown
          exit
          zone GMT
      exit
#-----
A:ALA-12>config>system#
```

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 on page 215](#)
 - [Name on page 216](#)
 - [Contact on page 216](#)
 - [Location on page 217](#)
 - [CLLI Code on page 217](#)
 - [Coordinates on page 218](#)
- [System Time Elements on page 219](#)
 - [Zone on page 219](#)
 - [Summer Time Conditions on page 221](#)
 - [NTP on page 222](#)
 - [SNTP on page 227](#)
 - [CRON on page 229](#)
 - [Time Range on page 232](#)
 - [Time of Day on page 236](#)
- [System Administration Parameters on page 241](#)
 - [Disconnect on page 242](#)
 - [Set-time on page 243](#)
 - [Display-config on page 243](#)
 - [Reboot on page 246](#)
 - [Save on page 245](#)

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 displayed below to configure the following system components:

- [System Information Parameters on page 216](#)
- [System Time Elements on page 219](#)

General system parameters include:

- [Name on page 216](#)
- [Contact on page 216](#)
- [Location on page 217](#)
- [CLLI Code on page 217](#)
- [Coordinates on page 218](#)

System Information Parameters

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: `alcatel>config>system# name ALA-12`

The following example displays the system name:

```
sysName@domain>config>system# info
#-----
echo "System Configuration "
#-----
      name "ALA-12"
. . .
      exit
#-----
sysName@domain>config>system#
```

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"`

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"`

CLLI Code

The Common Language Location Code (CLLI code) is an 11-character standardized geographic identifier that is used to uniquely identify the geographic location of a 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`

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 displays 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#
```

System Time Elements

The system clock maintains time according to Coordinated Universal Time (UTC). Configure information time zone and summer time (daylight savings time) parameters to correctly display time according to the local time zone.

Time elements include:

- Zone on page 219
- Summer Time Conditions on page 221
- NTP on page 222
- SNTP on page 227
- CRON on page 229
 - Time Range on page 232
 - Time of Day on page 236

Zone

The zone command sets the time zone and/or time zone offset for the device. The 7210-SAS OS supports system-defined and user-defined time zones. The system-defined time zones are listed in [Table 23](#).

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 displays the zone output:

```
A:ALA-12>config>system>time# info
-----
ntp
    server 192.168.15.221
    no shutdown
exit
snmp
    shutdown
exit
zone UTC
-----
A:ALA-12>config>system>time#
```

Table 23: 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
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

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 23](#), 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 23](#) or entered as optional parameters in this command.

The following example displays 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
```

NTP

Network Time Protocol (NTP) is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*. It allows for participating network nodes to keep time more accurately and maintain time in a synchronized manner between all participating network nodes.

NTP time elements include:

- [Authentication-check on page 222](#)
 - [Authentication-key on page 223](#)
 - [Broadcast on page 223](#)
 - [Broadcastclient on page 224](#)
 - [NTP-Server on page 225](#)
 - [Server on page 226](#)
-

Authentication-check

The authentication-check command provides for the option to skip the rejection of NTP PDUs that do not match the authentication key or authentication type requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type, or key.

When authentication-check is configured, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for key-id, one for type, and one for key value mismatches.

CLI Syntax: `config>system>time>ntp
authentication-check`

Example: `config>system>time>ntp#
config>system>time>ntp# authentication-check
config>system>time>ntp# no shutdown`

Authentication-key

This command configures an authentication key-id, key type, and key used to authenticate NTP PDUs sent to and received from other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, authentication type and authentication key value must match.

CLI Syntax: config>system>time>ntp
 authentication-key *key-id* {key *key*} [hash | hash2] type
 {des|message-digest}

Example: config>system>time>ntp#
 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 subnet.

CLI Syntax: config>system>time>ntp
 broadcast [router *router-name*] {interface
 ip-int-name> [key-id *key-id*] [version *version*]
 [ttl*t*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
```

Common Configuration Tasks

```
exit
A:sim1>config>system>time#
```

The following example in the config context shows NTP enabled with the broadcast command configured. At this level, the NTP broadcast commands are displayed at the end of the output after the router interfaces are shown.

```
A:sim1>config info

....

#-----
echo "System Time NTP Configuration"
#-----
system
time
ntp
broadcast interface toboth
exit
exit
exit
A:sim1>config
```

Broadcastclient

The `broadcastclient` command enables listening to NTP broadcast messages on the specified interface.

CLI Syntax: `config>system>time>ntp`
`broadcastclient[router router-name] {interface ip-int-name} [authenticate]`

Example: `config>system>time>ntp#`
`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
dst-zone PT
start second sunday april 02:00
end first sunday october 02:00
offset 0
exit
zone UTC
-----
A:ALA-12>config>system>time#
```


NTP-Server

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. If an authentication key-id is specified in this command, the NTP server requires client packets to be authenticated.

CLI Syntax: config>system>time>ntp
ntp-server [transmit *key-id*]

Example: config>system>time>ntp#
config>system>time>ntp# ntp-server transmit 1
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 five 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#
```

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 on page 227](#)
- [Server-address on page 228](#)

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#
```

CRON

The CRON command supports the Service Assurance Agent (SAA) functions as well as the ability to schedule turning on and off policies to meet “Time of Day” requirements. CRON functionality includes the ability to specify the commands that need to be run, when they will be scheduled, including one-time only functionality (oneshot), interval and calendar functions, as well as where to store the output of the results. In addition, CRON can specify the relationship between input, output and schedule. 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 elements include:

- [Action](#)
 - [Schedule](#)
 - [Script](#)
 - [Time Range](#)
 - [Time of Day](#)
-

Action

Parameters for a script including the maximum amount of time to keep the results from a script run, the maximum amount of time a script may run, the maximum number of script runs to store and the location to store the results.

CLI Syntax: `config>cron`

```

    action action-name [owner action-owner]
    expire-time {seconds|forever}
    lifetime {seconds|forever}
    max-completed unsigned
    results file-url
    script script-name [owner script-owner]
    shutdown
```

Example:`config>cron# action test`
`config>cron>action# results ftp://172.22.184.249/./sim1/test-results`
`config>cron>action# no shut`

The following example shows a script named “test” receiving an action to store its results in a file called “test-results”:

```

A:sim1>config>cron# info
-----
    script "test"
    location "ftp://172.22.184.249/./sim1/test.cfg"
```

```
        no shutdown
    exit
    action "test"
        results "ftp://172.22.184.249/./sim1/test-results"
        no shutdown
    exit
-----
A:sim1>config>cron# script
```

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.

CLI Syntax: config>cron

```
    schedule schedule-name [owner schedule-owner]
        action action-name [owner owner-name]
        count number
        day-of-month {day-number [..day-number] | all}
        description description-string
        end-time [date | day-name] time
        hour {hour-number [..hour-number] | all}
        interval seconds
        minute {minute-number [..minute-number] | all}
        month {month-number [..month-number] | month-name
            [..month-name] | all}
        no shutdown
        type {periodic | calendar | oneshot}
        weekday {weekday-number [..weekday-number] | day-name
            [..day-name] | all}
        shutdown
```

Example: config>cron# schedule test2

```
config>cron>sched# day-of-month 17
config>cron>sched# end-time 2007/07/17 12:00
config>cron>sched# minute 0 15 30 45
config>cron>sched# weekday friday
config>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>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>cron#

```

Script

The script command opens a new nodal context which contains information on a script.

CLI Syntax: config>cron

```

    script script-name [owner script-owner]
    description description-string
    location file-url
    shutdown

```

Example: config>cron# script test
config>cron>script#

The following example names a script “test”:

```

A:sim1>config>cron# info
-----
    script "test"
    location "ftp://172.22.184.249/./sim1/test.cfg"
    no shutdown
    exit
-----
A:sim1>config>cron#

```

Time Range

ACLs and QoS policy configurations may be enhanced to support time based matching. CRON configuration includes time matching with the 'schedule' sub-command. Schedules are based on events; time-range defines an end-time and will be used as a match criteria.

Time range elements include:

- [Create on page 232](#)
 - [Absolute on page 232](#)
 - [Daily on page 233](#)
 - [Weekdays on page 234](#)
 - [Weekend on page 234](#)
 - [Weekly on page 235](#)
-

Create

Use this command to enable the time-range context.

The following example creates a time-range called test1.

CLI Syntax: `config>cron>
 time-range name create`

Example: `config>cron# time-range test1 create
config>cron>time-range$`

Absolute

The absolute command configures a start and end time that will not repeat.

CLI Syntax: `config>cron>time-range$
 absolute absolute-time end absolute-time`

Example: `config>cron>time-range$ absolute start 2006/05/05,11:00 end
2006/05/06,11:01
config>cron>time-range$`

The following example shows an absolute time range beginning on May 5, 2006 at 11:00 and ending May 6, 2006 at 11:01:

```
A:sim1>config>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name       : test1
Triggers   : 0
Status     : Inactive
Absolute   : start 2006/05/05,11:00 end 2006/05/06,11:01
=====
A:sim1>config>cron>time-range#
```

Daily

The daily command configures the start and end of a periodic schedule for every day of the week (Sunday through Saturday).

CLI Syntax: config>cron>time-range\$
 daily start *time-of-day* end *time-of-day*

Example: config>cron>time-range\$ daily start 11:00 end 12:00
 config>cron>time-range\$

The following example shows a daily time range beginning at 11:00 and ending at 12:00.

```
A:sim1>config>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name       : 1
Triggers   : 0
Status     : Inactive
Periodic   : daily   Start 11:00 End 12:00
=====
A:sim1>config>cron>time-range#
```

Weekdays

The weekdays command configures the start and end of a periodic schedule for weekdays (Monday through Friday).

CLI Syntax: config>cron>time-range\$
 weekdays start *time-of-day* end *time-of-day*

Example: config>cron>time-range\$ weekdays start 11:00 end 12:00
 config>cron>time-range\$

The following command shows a time range beginning at 11:00 and ending at 12:00. This schedule runs all weekdays during this time period.

```
A:sim1>config>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name           : 1
Triggers       : 0
Status        : Inactive
Periodic      : weekdays Start 11:00 End 12:00
=====
A:sim1>config>cron>time-range#
```

Weekend

The weekend command configures the start and end of a periodic schedule for weekends (Saturday and Sunday). The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. A start time and end time of 11:00 is invalid.

CLI Syntax: config>cron>time-range\$
 weekend start *time-of-day* end *time-of-day*

Example: config>cron>time-range\$ weekend start 11:00 end 12:00
 config>cron>time-range\$

The following command shows a weekend time range beginning at 11:00am and ending at 12:00pm, both Saturday and Sunday.

To specify 11:00am to 12:00pm on Saturday or Sunday only, use the [Absolute](#) parameter for one day, or the [Weekly](#) parameter for every Saturday or Sunday accordingly. In addition, see the Schedule parameter to schedule oneshot or periodic events in the config>cron> context.

```
A:sim1>config>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name           : 1
Triggers       : 0
```

```
Status      : Inactive
Periodic    : weekend Start 11:00 End 12:00
```

Weekly

The weekly command configures the start and end of a periodic schedule for the same day every week, for example, every Friday. The start and end dates must be the same. The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. A start time and end time of 11:00 is invalid.

CLI Syntax: `config>cron>time-range$`
 weekly start *time-in-week* end *time-in-week*

Example: `config>cron>time-range$ start fri,01:01 end fri,01:02`
 `config>cron>time-range$`

The following command shows a weekly time range beginning on Friday at 1:01am ending Friday at 1:02am.

```
A:sim1>config>cron>time-range$ info
-----
        weekly start fri,01:01 end fri,01:02
-----
A:sim1>config>cron>time-range$
```

Time of Day

Time of Day (TOD) suites are useful when configuring many types of time-based policies or when a large number of subscribers or SAPs require the same type of TOD changes. The TOD suite may be configured while using specific ingress or egress ACLs or QoS policies, and is an enhancement of the ingress and egress CLI trees.

Time of day elements include:

- [SAPs on page 236](#)
 - [Egress on page 236](#)
 - [Ingress on page 238](#)
-

SAPs

- If a TOD Suite is assigned to a SAP, statistics collection are not collected for that SAP.
 - When an item is configured both on SAP level and in the TOD suite assigned to the SAP, the TOD-suite defined value takes precedence.
 - A policy or filter assignment configured directly on a SAP has a lower priority than any assignment in a TOD Suite. Hence, it is possible that a new direct configuration has no immediate effect. If the configuration is made by CLI, a warning is given.
-

Egress

This command is an enhancement for specific egress policies. Use this command to create time-range based associations of previously created filter lists, QoS and scheduler policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range.

Filters

In a TOD suite, filters that have entries with time-ranges may not be selected. Similarly, filter entries with a time-range may not be created while a TOD suite refers to that filter. QoS policies and filters referred to by a TOD suite must have scope “template” (default).

The following syntax is used to configure TOD-suite egress parameters.

CLI Syntax:

```

config
  cron
    tod-suite tod-suite-name create
      egress
        filter ip ip-filter-id [time-range time-range-name]
          [priority priority]
        filter mac mac-filter-id [time-range time-range-name]
          [priority priority]

```

Example:

```

config>cron>tod-suite$ egress filter ip 100
config>cron>tod-suite$

```

The following command shows an egress IP filter association with filter ID 100.

```

sim1>config>filter# ip-filter 100 create
A:sim1>config>filter>ip-filter$ entry 10 create
A:sim1>config>filter>ip-filter>entry$
A:sim1>config>cron>tod-suite# egress filter ip 100
A:sim1>config>cron>tod-suite# info detail
-----
      no description
      egress
        filter ip 100
      exit
-----
A:sim1>config>cron>tod-suite#

```

Ingress

This command is an enhancement for specific ingress policies including filter lists and QoS policies. Use this command to create time-range based associations of previously created filter lists QoS policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range. To configure a daily time-range across midnight, use a combination of two entries. An entry that starts at hour zero will take over from an entry that ends at hour 24.

CLI Syntax:

```
config>system
      cron
        tod-suite tod-suite-name create
          ingress
            filter ip ip-filter-id [time-range time-range-name]
              [priority priority]
            filter mac mac-filter-id [time-range time-range-name] [priority priority]
            qos policy-id [time-range time-range-name] [priority priority]
```

Example:

```
config>cron>tod-suite$ ingress filter ip 100
config>cron>tod-suite$
```

The following command shows an ingress IP filter association with filter ID 100.

```
sim1>config>filter# ip-filter 100 create
A:sim1>config>filter>ip-filter$ entry 10 create
A:sim1>config>filter>ip-filter>entry$
...
A:sim1>config>cron>tod-suite# ingress filter ip 100
A:sim1>config>cron>tod-suite# info detail
-----
      no description
      ingress
        filter ip 100
      exit
-----
A:sim1>config>cron>tod-suite#
```

Example: config>cron>tod-suite\$ ingress qos 101
config>cron>tod-suite\$

The following command shows an association with ingress QoS-SAP policy 101.

```
A:sim1>config>qos# sap-egress 101 create
...
A:sim1>config>cron>tod-suite# ingress qos 101
A:sim1>config>cron>tod-suite# info detail
-----
      no description
      ingress
        qos 101
      exit
-----
A:sim1>config>cron>tod-suite#
```

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 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"
      clli-code "abcdefgl234"
      coordinates "N 45 58 23, W 34 56 12"
      config-backup 7
...
#-----
A:ALA-12>config>system>time#
```


System Administration Parameters

Use the CLI syntax displayed below to configure various system administration parameters.

Administrative parameters include:

- [Validating the Golden Bootstrap Image on page 241](#)
 - [Updating the Golden Bootstrap Image on page 242](#)
 - [Disconnect on page 242](#)
 - [Set-time on page 243](#)
 - [Display-config on page 243](#)
 - [Save on page 245](#)
 - [Reboot on page 246](#)
 - [Post-Boot Configuration Extension Files on page 247](#)
-

Validating the Golden Bootstrap Image

The **admin>check-golden-bootstrap** command validates the current golden bootstrap image, and displays its version. A default golden bootstrap image is installed on every 7210 SAS E unit.

CLI Syntax: admin
 check-golden-bootstrap

Example: admin# check-golden-bootstrap

The following example displays the output.

```
version TiMOS-L-0.0.I312
Golden Bootstrap Image validation successful
```

Updating the Golden Bootstrap Image

The **admin>update-golden-bootstrap** command validates the input file, which must be a 7210 SAS E bootstrap image, and updates the golden bootstrap image with the contents of this file.

Note: Only on 7210 SAS-D newer platforms, the **admin>update-golden-bootstrap** CLI command does not update the golden-bootstrap image with the boot.tim specified in the parameter value, if the boot.tim is not a new image.

CLI Syntax: admin
 update-golden-bootstrap [<file-url>]

Example: admin# update-golden-bootstrap boot.tim

The following is an example of the output.

```
Updating Golden Bootstrap Image from "boot.tim"
This operation must not be interrupted
Updating Golden Bootstrap image .... Completed.
```

Disconnect

The **disconnect** command immediately disconnects a user from a console, Telnet, FTP, or SSH session.

Note: Configuration modifications are saved to the primary image file.

CLI Syntax: admin
 disconnect [address *ip-address* |username *user-name* |
 {console|telnet|ftp|ssh}]

Example: admin# disconnect

The following example displays the disconnect command results.

```
ALA-1>admin# disconnect
ALA-1>admin# Logged out by the administrator
Connection to host lost.

C:\>
```

Set-time

Use the **set-time** command to set the system date and time. The time entered should be accurate for the time zone configured for the system. The system will convert the local time to UTC before saving to the system clock which is always set to UTC. If SNTP or NTP is enabled (no shutdown) then this command cannot be used. The set-time command does not take into account any daylight saving offset if defined.

CLI Syntax: admin
 set-time *date time*

Example: admin# set-time 2007/02/06 04:10:00

The following example displays the set-time command results.

```
ALA-2# admin set-time 2007/02/06 04:10:00
ALA-2# show time
Thu Feb 2 04:10:04 GMT 2007
ALA-2#
```

Display-config

The **display-config** command displays the system's running configuration.

CLI Syntax: admin
 display-config [detail] [index]

Example: admin# display-config detail

The following example displays a portion of the **display-config detail** command results.

```
A:ALA-12>admin# display-config detail
#-----
echo "System Configuration"
#-----
system
  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"
  config-backup 7
  boot-good-exec "ftp://test:test@192.168.xx.xxx/./lxx.cfg.A"
  boot-bad-exec "ftp://test:test@192.168.xx.xxx/./lxx.cfg.1"
  lacp-system-priority 1
  no synchronize
  snmp
    shutdown
    engineID "0000197f000000000467ff00"
```

System Administration Parameters

```
        packet-size 1500
        general-port 161
exit
login-control
    ftp
        inbound-max-sessions 3
    exit
    telnet
        inbound-max-sessions 5
        outbound-max-sessions 2
    exit
    idle-timeout 1440
    pre-login-message "Property of Service Routing Inc.Unauthorized access prohib-
ited."
    motd text "Notice to all users: Software upgrade scheduled 3/2 1:00 AM"
exit
security
    management-access-filter
        default-action permit
    entry 1
        no description
...
```

Tech-support

The `tech-support` command creates a system core dump. **NOTE:** This command should only be used with explicit authorization and direction from Alcatel-Lucent's Technical Assistance Center (TAC).

Save

The `save` command saves the running configuration to a configuration file. When the `debug-save` parameter is specified, debug configurations are saved in the config file. If this parameter is not specified, debug configurations are not saved between reboots.

CLI Syntax: `admin`
 `save [file-url] [detail] [index]`
 `debug-save [file-url]`

Example: `admin# save ftp://test:test@192.168.x.xx/./1.cfg`
 `admin# debug-save debugsave.txt`

The following example displays the `save` command results.

```
A:ALA-1>admin# save ftp://test:test@192.168.x.xx/./1x.cfg
Writing file to ftp://test:test@192.168.x.xx/./1x.cfg
Saving configuration ...Completed.
ALA-1>admin# debug-save ftp://test:test@192.168.x.xx/./debugsave.txt
Writing file to ftp://julie:julie@192.168.x.xx/./debugsave.txt
Saving debug configuration .....Completed.
A:ALA-1>admin#
```

Reboot

The **reboot** command reboots the router including redundant cards in redundant systems. If the **now** option is not specified, you are prompted to confirm the reboot operation.

CLI Syntax: `admin
 reboot [auto-init][now]`

Example: `admin# reboot now`

The following example displays the **reboot** command results.

```
A:ALA-1>admin# reboot now
Are you sure you want to reboot (y/n)? y
Rebooting...
Using preloaded VxWorks boot loader.
...
```

When an **admin reboot auto-init** command is issued, the system resets the existing BOF file and reboots. The system startup process after the **admin reboot auto-init** command is executed is the same as the first time system boot as described in [System Initialization on page 108](#).

NOTE: Since the BOF is reset, the system may not boot up with the last saved system configuration unless the new BOF file also uses the same configuration file. If it is required that the system boot up with the last saved system configuration, it is recommended to use the **admin>save file-url** command to save the current system configuration and modify the BOF to use this.

Use the following CLI to reset the BOF and reboot:

CLI Syntax: `admin# reboot auto-init [now]`
Example: `*A:ALA-1# admin reboot auto-init`
WARNING: Configuration and/or Boot options may have changed since the last save.
Are you sure you want to reset the bof and reboot (y/n)? Y
Resetting...OK

```
Alcatel-Lucent 7210 Boot ROM. Copyright 2000-2008 Alcatel-Lucent.
All rights reserved. All use is subject to applicable license agreements.
```

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 displays the command output:

```
*A:ALA# configure system
*A:ALA>config>system# info
-----
#-----
echo "System Configuration"
#-----
name "ALA"
boot-good-exec "cf1:\good.cfg"
boot-bad-exec "cf1:\bad.cfg"
snmp
shutdown
exit
login-control
idle-timeout disable
pre-login-message "ala-1" name
exit
time
ntp
authentication-key 1 key "SV3BxZCsIvI" hash type message-digest
server 10.135.16.130
peer 21.0.0.1 key-id 1
no shutdown
exit
snmp
server-address 10.135.16.90 preferred
no shutdown
exit
zone UTC
exit
thresholds
rmon
exit
exit
```

System Administration Parameters

```
#-----
echo "System Security Configuration"
#-----
    security
        hash-control read-version all write-version 1
        telnet-server
        ftp-server
        snmp
            community "private" rwa version both
            community "public" r version both
        exit
        source-address
            application ftp 10.135.16.97
            application snmptrap 10.135.16.97
            application ping 10.135.16.97
            application dns 10.135.16.97
        exit
    exit
-----
*A:ALA>config>system#
```


Show Command Output and Console Messages

The `show>system>information` command displays the current value of the bad/good exec URLs and indicates whether a post-boot configuration extension file was executed when the system was booted. If an extension file was executed, the `show>system>information` command also indicates if it completed successfully or not.

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/./12.cfg' ...
System Configuration
Log Configuration
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./12.cfg, Line 195: Command "log" failed.
CRITICAL: CLI #1002 An error occurred while processing the configuration file.
The system configuration is missing or incomplete.
MAJOR: CLI #1008 The SNMP daemon is disabled.
If desired, enable SNMP with the 'config>system>snmp no shutdown' command.
Attempting to exec configuration failure extension file:
'ftp://test:test@192.168.xx.xxx/./fail.cfg' ...
Config fail extension
Enabling SNMP daemon
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./fail.cfg, Line 5: Command "abc log" failed.
TiMOS-B-x.0.Rx both/hops ALCATEL Copyright (c) 2000-2001 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Thu Nov 20 19:19:11 PST 2008 by builder in /rel5x.0/b1/Rx/panos/main

Login:
```

System Timing

When synchronous Ethernet is enabled, the operator can select an Ethernet port as a candidate for timing reference. The timing information recovered from this port is used to time the system.

Note: In the current release the derived time is distributed only through other Ethernet ports.

```
CLI Syntax:
config>system>sync-if-timing
    abort
    begin
    commit
    ref-order first second
    refl
        source-port port-id
        no shutdown
    ref2
        source-port port-id
        no shutdown
    no revert
```

Edit Mode

To enter the mode to edit timing references, you must enter the **begin** keyword at the **config>system>sync-if-timing#** prompt.

Use the following CLI syntax to enter the edit mode:

```
CLI Syntax: config>system>sync-if-timing
               begin
```

The following error message displays when the you try to modify **sync-if-timing** parameters without entering the keyword **begin**.

Note: Use the option commit to save or abort to discard the changes made in a session.

```
ort 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 refl to 2/1/1.
A:ALA-12>config>system>sync-if-timing>refl#
```

Configuring Timing References

Configuration Guidelines

Ref1 has to be configured to use one of the ports from 1/1/1 up to 1/1/4 and ref2 should be configured to use either 1/1/5 or 1/1/6. The software enforces this check. The ports 1/1/7 up to 1/1/10 can be configured as either ref1 or ref2.

Listed below is an example to configure timing reference parameters.

Example:

```
config>system# sync-if-timing
config>system>sync-if-timing# begin
config>system>sync-if-timing# ref1
config>system>sync-if-timing>ref1# source-port 1/1/1
config>system>sync-if-timing>ref1# no shutdown
config>system>sync-if-timing>ref1# exit
config>system>sync-if-timing# ref2
config>system>sync-if-timing>ref2# source-port 1/1/2
config>system>sync-if-timing>ref2# no shutdown
config>system>sync-if-timing>ref2# exit
config>system>sync-if-timing>commit
```

The following displays the timing reference parameters:

```
*7210-SAS>config>system>sync-if-timing#info detail
```

```
-----
ref-order ref1 ref2
ref1
    source-port 1/1/1
    no shutdown
exit
ref2
    source-port 1/1/2
    no shutdown
exit
no revert
-----
```

Using the Revert Command

If the current reference goes offline or becomes unstable the revert command allows the clock to **revert** to a higher-priority reference.

When revert is 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
```

Configuring System Monitoring Thresholds

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.

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.

Configuring System Monitoring Thresholds

To create events, use the following CLI:

Example: config>system>thresholds# cflash-cap-warn cf1-B: rising-threshold 2000000 falling-threshold 1999900 interval 240 trap startup-alarm either

Example: config>system>thresholds# memory-use-alarm rising-threshold 50000000 falling-threshold 45999999 interval 500 both startup-alarm either

Example: config>system>thresh# rmon

Example: config>system>thresh>rmon# event 5 both description "alarm testing" owner "Timos CLI"

The following example displays 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#
```

System Alarm Contact Inputs in 7210 SAS-E devices

The 7210 SAS E platform hardware supports alarm contact inputs that allow an operator to monitor and report changes in the external environmental conditions. In a remote or outdoor deployment, alarm contact inputs allow an operator to detect conditions, for example, air conditioner fault, open door.

An operator can configure generation of events when alarm contact inputs transition between the open and close states. For each generated event, the operator can specify the:

- Action associated with each state transition.
- Severity associated with each state transition.
- Log message associated with each state transition.

Configuring LLDP

The following output displays LLDP defaults:

```
A:7210-SAS>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
-----
```

The following example displays an LLDP port configuration:

```
*A:7210-SAS>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:7210-SAS>config>port>ethernet>lldp#
```

The following example displays a global system LLDP configuration:

```
A:7210-SAS>config>system>lldp# info
-----
tx-interval 10
tx-hold-multiplier 2
reinit-delay 5
notification-interval 10
-----
A:7210-SAS>config>system>lldp#
```


System Resource Allocation

Allocation of Ingress Internal TCAM resources

In current releases, the system statically allocates ingress TCAM resources for use by SAP ingress QoS classification, SAP ingress access control list (ACLs), Identifying and sending CFM OAM packets to CPU for local processing, and so on. The resource allocation is not user configurable. With introduction of new capabilities such as IPv6 classification, UP MEP support, and G8032-fast-flood, the static allocation of resources by software does not meet requirements of different customers, who typically want to use different features.

The user can allocate a fixed amount of resources per system to be used for QoS, ACLs, CFM/Y.1731 MEPs and other features. Some of these parameters are boot-time and others are run-time. A change in current value of the parameter that is designated 'boot-time' needs a reboot of the node, before the new value takes effect. Change in current value of the parameter that is designated 'run-time' takes effect immediately, if the software determines resources are available for use to accommodate the change.

During system bootup, the system reads all the resource profile parameters and allocates resources to the features, in the order of which it appears in the configuration file. (NOTE: The order in which the command appears in the configuration file is important). The resources are shared; therefore the user has to ensure that the sum total of such resources does not exceed the limit supported by the platform. If the system determines that it cannot allocate the requested resources, the system disables the feature from use. For example, if the system determines that it cannot allocate resources for g8032-fast-flood, it disables the feature from use (that is, G8032 eth-rings does not use fast-flood mechanisms). Another example is, if the system determines that it cannot allocate resources for ipv4-based SAP Ingress ACL classification, then the system does not allow users to use ipv4-based SAP ingress ACL classification feature and fails the configuration when it comes upon the first SAP in the configuration file which uses an IPv4-based SAP ingress ACL policy.

For boot-time parameters, such as g8032-fast-flood-enable, it is the user's responsibility to ensure that configuration of services matches the resource allocated. If the system determines that it cannot allocate resources to services then it fails the configuration file at the first instance where it encounters a command to which resources cannot be allocated. The available resources can be allocated to different features. Please refer to the scaling guide for amount of resources available per platform and per feature.

For ACL and QoS resources, the user has the option to allocate resources to limit usage per feature, irrespective of the match criteria used (that is, sum of all resources used for different SAP ingress classification match-criteria is limited by the amount allocated for SAP ingress classification) and can further allocate resources for use by specific match criteria. User can enable any of the match criteria from among those supported and associate a fixed amount of resources with each of them in are put together of fixed sizes (the chunk size is dependent on the platform).

The system attempts to allocate resources in order it appears in the configuration file and fails any match criteria if it does not have any more resources to allocate. User is also provided with a keyword 'max' to indicate that the system needs to allocate resources when it is first required, as long as the maximum resources allocated for that feature is not exceeded or maximum resource available in the system is not exceeded. 7210 platforms allocates resources to each of the features and the match-criteria in fixed size chunks, on priority basis.

The no forms of the command disables the use of corresponding match criteria. During runtime, the command succeeds, if no SAPs are currently using the criteria. Similarly, reduction of resources from the current value to a lower value succeeds, if no SAPs are currently using the criteria. If the system can successfully execute the command, it can free up the resources which were in use by that slice or chunk and makes it available for use by other features. This implies the user either deletes a SAP or removes the ingress ACL policy association with a SAP to free up resources. By executing these commands the system releases some entries in a given chunk or releases an entire chunk. If an entire chunk is freed, it is returned to the system free pool for use by other features. If some entries in the chunk are freed, it is made available for use by other SAPs using the same feature to which the chunk has been allocated to.

The 'no' form of the commands which are designated as boot-time does not take effect immediately. It takes effect after the reboot. Before reboot it is the user's responsibility to free up resources required for use by the feature which has been enabled to take effect after the reboot. By not doing so, results in failure when the configuration file is executed on boot up.

For more details about individual commands and features that use System Resource Allocation. Please see the CLI descriptions and the feature description in the respective user guides.

Allocation of Egress Internal TCAM resources

Note: Supported only on 7210 SAS-D. It is not available on 7210 SAS-E.

In the current releases, the system statically allocates egress TCAM resources for use by different criteria in SAP egress access control list (ACLs) and other purposes. The resource allocation is not user configurable. With introduction of new capabilities such as IPv6 match criteria in egress, the static allocation of resources by software does not meet requirements of different customers, who typically want to use different features. Therefore, ingress internal TCAM resource allocation capabilities has been extended to the egress internal TCAM resources.

For more details about individual commands and features that use System Resource Allocation. Please see the CLI descriptions and the feature description in the respective user guides.

NOTE: Boot-time commands under the `config> system> resource-profile` will not take effect when a configuration file is executed using the 'exec' CLI command. Boot-time commands under the `config> system> resource-profile` are read and acted upon by the system only during boot.

System Resource Allocation Examples

Example one:

```
config> system> resource-profile
...
acl-sap-ingress 3
    mac-match-enable max
    ipv4-match-enable 1
    no ipv6_128-ipv4-match-enable
    no ipv6_64-only-match-enable
exit
...
```

In the above example CLI, the system takes the following actions:

- System allocates 3 chunks for use by the SAP ingress ACL entries.
- System allocates 1 chunk for use by SAP ingress ACL entries using ipv4-criteria. The system fails the configuration when the number of ACL entries using ipv4-criteria exceeds the configured limit (that is, the system does not allocate in excess of the configured limit of 1 chunk).
- System allocates a chunk for use by SAP ingress ACL entries using mac-criteria. The system initially allocates 1 chunk for use by SAPs that use ingress ACLs with mac-criteria. The system can allocate more chunks, up-to 2 chunks, as the user has specified the 'max' keyword. More chunks are allocated when user configures SAP that use mac-criteria and all of the entries in the allocated chunk(s) is used up. The system fails the configuration when the number of ACL entries with mac-criteria exceeds the limit of 2 chunks allocated to SAP ingress ACL match (that is, the system does not allocate in excess of the configured limit of 3 chunks = up-to 2 for mac-criteria and 1 for ipv4-criteria).
- The system fails user attempt to use SAP ingress ACLs with ipv6 match criteria (and the other combinations listed above), as the user has disabled the use of these criteria.

Example 2:

```
config> system> resource-profile>ingress-internal-tcam>
...
acl-sap-ingress 3
    mac-match-enable max
    ipv4-match-enable 1
    no ipv6_128-ipv4-match-enable
    ipv6_64-only-match-enable max
exit
...
```

In the above example CLI, the system will take the following actions:

- System allocates 3 chunks for use by the SAP ingress ACL entries.

- System allocates 1 chunk for use by SAP ingress ACL entries using ipv4-criteria. The system fails the configuration when the number of ACL entries using ipv4-criteria exceeds the configured limit (that is, the system does not allocate in excess of the configured limit of 1 chunk).
- System allocates a chunk for use by SAP ingress ACL entries using mac-criteria. The system initially allocates 1 chunk for use by SAPs that use ingress ACLs with mac-criteria. The system can allocate more chunks, as the user has specified the 'max' keyword, if a chunk is available for use. In this particular example, as there are no more chunks available, mac-criteria cannot allocate more than 1 chunk (even though it specifies the max keyword). The system fails the configuration when the number of ACL entries with mac-criteria exceeds the limit of 1 chunks allocated to SAP ingress ACL mac-criteria (that is, the system does not allocate in excess of the configured limit of 3 chunks = 1 for mac-criteria + 1 for ipv4-criteria + 1 for ipv6-criteria).
- System allocates a chunk for use by SAP ingress ACL entries using ipv6-64-bit criteria. The system initially allocates 1 chunk for use by SAPs that use ingress ACLs with ipv6-64-bit criteria. The system can allocate more chunks, as the user has specified the 'max' keyword. In this particular example, as there are no more chunks available, ipv6-64-bit criteria cannot allocate more than 1 chunk (even though it specifies the max keyword). The system fails the configuration when the number of ACL entries with ipv6-64-bit criteria exceeds the limit of one chunk allocated to SAP ingress ACL match (that is, the system does not allocate in excess of the configured limit of 3 chunks = 1 for mac-criteria + 1 for ipv4-criteria + 1 for ipv6-64-bit criteria).
- The system fails the user attempt to use SAP ingress ACLs with ipv6-128 bit match criteria (and the other combinations listed above), as the user has disabled use of these criteria.

In the example-2 above, the user can execute `no ipv4-match-enable` to disable use of ipv4-criteria. The system checks if there are SAPs using ipv4-criteria and fails the command if one exists; else it the chunk freed, is for use with either mac-criteria or ipv6-64-bit criteria. The entire chunk is allocated to mac-criteria, if the first SAP that needs resources requests for mac-criteria and there are no entries in the chunk already allocated to mac-criteria, leaving no more resources for use by ipv6-64-bit criteria or the entire chunk is allocated to ipv6-64-bit criteria, if the first SAP that needs resources requests for ipv6-64-bit criteria and there are no entries in the chunk already allocated to ipv6-64-bit criteria, leaving no resources for use by mac-criteria.

System Command Reference

Command Hierarchies

Configuration Commands

- [System Information Commands on page 261](#)
- [System Alarm Commands on page 263](#)
- [PTP Commands on page 262](#)
- [System Time Commands on page 265](#)
- [Cron Commands on page 266](#)
- [System Administration \(Admin\) Commands on page 267](#)
- [System Alarm Contact Commands on page 268](#)
- [LLDP System Commands on page 270](#)
- [LLDP Ethernet Port Commands on page 270](#)
- [System Resource-Profile Commands for 7210 SAS-D on page 271](#)
- [Fan Controller Commands for 7210 SAS-D and 7210 SAS-D ETR variant with 128MB flash on page 273](#)
- [Show Commands on page 274](#)
- [Debug Commands on page 275](#)
- [Clear Commands on page 275](#)

System Information Commands

```

config
— system
— alarm-contact-input alarm-contact-input-id (supported only on 7210 SAS E)
— boot-bad-exec file-url
— no boot-bad-exec
— cli-code cli-code
— no cli-code
— config-backup count
— no config-backup
— contact contact-name
— no contact
— coordinates coordinates
— no coordinates
— lacp-system-priority lacp-system-priority
— no lacp-system-priority
— lldp
— location location
— no location

```

Command Hierarchies

- **login-control**
- **name** *system-name*
- **no name**
- **power-supply** [*power-supply-id*] *type* (supported only on 7210 SAS-D ETR)
- **[no] vwm-shelf** *vwm-shelf-id* **[create]** (Supported only on 7210 SAS-E)
 - **[no] shutdown**

System Alarm Commands

```

config
  — system
    — thresholds
      — cflash-cap-alarm cflash-id rising-threshold threshold [falling-threshold threshold]
        interval seconds [rmon-event-type] [startup-alarm alarm-type]
      — no cflash-cap-alarm cflash-id
      — cflash-cap-warn cflash-id rising-threshold threshold [falling-threshold threshold]
        interval seconds [rmon-event-type] [startup-alarm alarm-type]
      — no cflash-cap-warn cflash-id
      — memory-use-alarm rising-threshold threshold [falling-threshold threshold] interval
        seconds [rmon-event-type] [startup-alarm alarm-type]
      — no memory-use-alarm
      — memory-use-warn rising-threshold threshold [falling-threshold threshold] interval
        seconds [rmon-event-type] [startup-alarm alarm-type]
      — no memory-use-warn
      — [no] rmon
        — alarm rmon-alarm-id variable-oid oid-string interval seconds [sample-type]
          [startup-alarm alarm-type] [rising-event rmon-event-id rising-threshold
            threshold] [falling event rmon-event-id falling-threshold threshold] [owner
            owner-string]
        — no alarm rmon-alarm-id
        — event rmon-event-id [event-type] [description description-string] [owner
          owner-string]
        — no event rmon-event-id

```

PTP Commands (applicable only to 7210 SAS-D ETR)

```
config
  — system
    — ptp
      — clock-type boundary
      — clock-type ordinary {slave}
      — [no] domain domain
      — [no] log-sync-interval value
      — network-type {sonet|sdh}
      — [no] peer ip-address [create]
        — [no] priority local-priority
        — [no] shutdown
      — profile {g8265dot1-2010|ieee1588-2008}
        — [no] priority1 priority-value
        — [no] priority2 priority-value
      — [no] shutdown
```


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
        — [no] broadcast [router router-name] {interface ip-int-name} [key-id key-id]
          [version version] [ttl ttl]
        — [no] broadcast [router router-name] {interface ip-int-name}
        — broadcastclient [router router-name] {interface ip-int-name} [authenticate]
        — [no] broadcastclient [router router-name] {interface ip-int-name}
        — [no] ntp-server [transmit key-id]
        — [no] peer ip-address [version version] [key-id key-id] [prefer]
        — [no] server ip-address [version version] [key-id key-id] [prefer]
        — [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

```

Cron Commands

```

config
— [no] cron
    — [no] action action-name [owner owner-name]
        — expire-time {seconds | forever}
        — lifetime {seconds | forever}
        — max-completed unsigned
        — [no] results file-url
        — [no] script script-name [owner owner-name]
        — [no] shutdown
    — [no] schedule schedule-name [owner owner-name]
        — [no] action action-name [owner owner-name]
        — [no] day-of-month {day-number [..day-number] all}
        — count number
        — [no] description description-string
        — [no] end-time [date|day-name] time
        — [no] hour {..hour-number [..hour-number] all}
        — [no] interval seconds
        — [no] minute {minute-number [..minute-number] all}
        — [no] month {month-number [..month-number] month-name [..month-name] all}
        — [no] shutdown
        — type {schedule-type}
        — [no] weekday {weekday-number [..weekday-number] day-name [..day-name] all}
    — [no] script [no] script script-name [owner owner-name]
        — [no] description description-string
        — [no] location file-url
        — [no] shutdown
    — [no] time-range name [create]
        — absolute start start-absolute-time end end-absolute-time
        — no absolute start start-absolute-time
        — daily start start-time-of-day end end-time-of-day
        — no daily start start-time-of-day
        — [no] description description-string
        — weekdays start start-time-of-day end end-time-of-day
        — no weekdays start start-time-of-day
        — weekend start start-time-of-day end end-time-of-day
        — no weekend start start-time-of-day
        — weekly start start-time-in-week end end-time-in-week
        — no weekly start start-time-in-week
    — [no] tod-suite <tod-suite-name> [create]
        — egress
            — filter ip ip-filter-id [time-range time-range-name] [priority priority]
            — filter mac mac-filter-id [time-range time-range-name] [priority priority]
            — no filter ip ip-filter-id [time-range time-range-name]
            — no filter mac mac-filter-id [time-range time-range-name]
        — ingress
            — filter ip ip-filter-id [time-range time-range-name] [priority priority]
            — filter mac mac-filter-id [time-range time-range-name] [priority priority]
            — no filter ip ip-filter-id [time-range time-range-name]
            — no filter mac mac-filter-id [time-range time-range-name]
            — qos policy-id [time-range time-range-name] [priority priority]
            — no qos policy-id [time-range time-range-name]

```

System Administration (Admin) Commands

```
root
— admin
  — check-golden-bootstrap
  — debug-save file-url
  — disconnect {address ip-address | username user-name | console | telnet | ftp | ssh}
  — display-config [detail | index]
  — [no] enable-tech
  — reboot [upgrade][auto-init] [now]
  — save [file-url] [detail] [index]
  — set-time <date> <time>
  — tech-support [file-url]
  — update-golden-bootstrap [file-url]
```

System Alarm Contact Commands

Note: System alarm contact commands are not supported on 7210 SAS-D devices.

```
config
— system
  — alarm-contact-input alarm-contact-input-id
    — [no] alarm-output-severity [critical | major | minor | none]
    — [no] clear-alarm-msg {alarm-msg-txt}
    — description description-string
    — normal-state [open | closed]
    — [no] shutdown
    — [no] trigger-alarm-msg {alarm-msg-txt}
```

System Synchronization Commands

```

config
  — system
    — sync-if-timing
      — abort
      — begin
      — commit
      — ref-order first second
      — no ref-order
      — ref1
        — ql-override {prs | stu | st2 | tnc | st3e | st3 | prc | ssua | ssub | sec | eec1 | eec2}
        — no ql-override
        — [no] shutdown
        — source-port port-id
        — no source-port
      — ref2
        — ql-override {prs | stu | st2 | tnc | st3e | st3 | prc | ssua | ssub | sec | eec1 | eec2}
        — no ql-override
        — [no] shutdown
        — source-port port-id
        — no source-port
      — [no] ql-selection
      — [no] revert
  
```

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
```

LLDP Ethernet Port Commands

```
configure
  — port port-id
    — ethernet
      — lldp
        — dest-mac {nearest-bridge | nearest-non-tpmr | nearest-customer}
          — admin-status {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
```

System Resource-Profile Commands for 7210 SAS-D

```

configure
  — system
    — resource-profile
      — egress-internal-team
        — acl-sap-egress [num-resources]
        — no acl-sap-egress
          — [no] ipv6-128bit-match-enable num-resources
          — mac-ipv4-match-enable num-resources
          — no mac-ipv4-match-enable
          — mac-ipv6-64bit-match-enable num-resources
          — no mac-ipv6-64bit-match-enable
          — mac-match-enable num-resources
          — no mac-match-enable
      — ingress-internal-team
        — acl-sap-ingress [num-resources]
        — no acl-sap-ingress
          — ipv4-ipv6-128-match-enable num-resources
          — no ipv4-ipv6-128-match-enable
          — ipv4-match-enable num-resources
          — no ipv4-match-enable
          — ipv6-64-only-match-enable num-resources
          — no ipv6-64-only-match-enable
          — mac-match-enable num-resources
          — no mac-match-enable
          — eth-cfm [num-resources]
          — no eth-cfm
          — up-mep num-resources
          — no up-mep
        — no qos-sap-ingress-resource
        — qos-sap-ingress-resource num-resources
          — ipv4-match-enable num-resources
          — no ipv4-match-enable
          — ipv6-ipv4-match-enable num-resources
          — no ipv6-ipv4-match-enable
          — mac-match-enable num-resources
          — no mac-match-enable
        — no sap-aggregate-meter
        — sap-aggregate-meter num-resources
      — [no] max-ipv6-routes number

```

System Resource-Profile Commands for 7210 SAS-E

```
configure
  — system
    — resource-profile
      — ingress-internal-tcam
        — acl-sap-ingress [num-resources]
        — no acl-sap-ingress
          — ipv4-ipv6-128-match-enable num-resources
          — no ipv4-ipv6-128-match-enable
          — ipv4-match-enable num-resources
          — no ipv4-match-enable
          — ipv6-64-only-match-enable num-resources
          — no ipv6-64-only-match-enable
          — mac-match-enable num-resources
          — no mac-match-enable
        — dhcp-snooping-enable
        — no dhcp-snooping-enable
        — no qos-sap-ingress-resource
        — qos-sap-ingress-resource num-resources
          — ipv4-match-enable num-resources
          — no ipv4-match-enable
          — ipv6-ipv4-match-enable num-resources
          — no ipv6-ipv4-match-enable
          — mac-match-enable num-resources
          — no mac-match-enable
```


Fan Controller Commands for 7210 SAS-D and 7210 SAS-D ETR variant with 128MB flash

```
configure
  — system
    — fan {on | off | auto}
```

Show Commands

show

- **alarm-contact-input** *alarm-contact-input-id* **detail** (supported only on 7210 SAS-E)
- **alarm-contact-input** **all** (supported only on 7210 SAS-E)
- **chassis** [**environment**] [**power-supply**] (The ‘environment’ option is supported only on 7210 SAS-E and 7210 SAS-D. The ‘power-supply’ option is applicable only to 7210 SAS-D ETR)
- **cron**
 - **action** *action-name* [**owner** *owner-name*]
 - **action** *run-history* [*run-state*]
 - **schedule** *action-name* [**owner** *owner-name*]
 - **script** *script-name* [**owner** *owner-name*]
 - **tod-suite** *tod-suite-name* [**detail**] **associations** **failed-associations**
 - **time-range** *name* **associations** [**detail**]
- **time**
- **system**
 - **connections** [**address** *ip-address* [**port** *port-number*] [**detail**]
 - **cpu** [**sample-period** *seconds*]
 - **information**
 - **lldp**
 - **lldp** **neighbor**
 - **memory-pools**
 - **ntp**
 - **resource-profile** [**active**|**configured**]
 - **ptp** [**peer** <*ip-address*> [**detail**] | **peers** [**detail**] | **unicast** | **statistics** | **standby** |
 - **sntp**
 - **sync-if-timing**
 - **thresholds**
 - **time**
 - **vwm-shelf** *vwm-shelf-id* [**all**] [**detail**] (Supported only on 7210 SAS-E)
- **uptime**
- **alarm-contact-input** *alarm-contact-input-id* [**detail**] (Supported only on 7210 SAS-E)
- **alarm-contact-input** **all** (Supported only on 7210 SAS-E)

Clear Commands

```
clear
  — cron
    — action
      — completed [action-name] [owner action-owner]
  — screen
  — system
    — sync-if-timing {ref1 | ref2}
```

Debug Commands

```
debug
  — sync-if-timing
    — force-reference {ref1 | ref2}
    — no force-reference
  — [no] system
    — ntp [router router-name] [interface ip-int-name]
```

Fan controller debug command (applicable only to 7210 SAS-D and 7210 SAS-D ETR variant with 128MB flash)

```
tools
  — dump
    — fan-stats
```

System Command Reference Descriptions

Generic Commands

shutdown

Syntax	[no] shutdown
Context	config>system>time>ntp config>system>time>sntp config>cron>action config>cron>sched config>cron>script
Description	This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted. The no form of this command places the entity into an administratively enabled state.
Default	no shutdown

description

Syntax	description <i>description-string</i> no description
Context	config>cron>sched
Description	This command creates a text description stored in the configuration file for a configuration context. The description command associates a text string with a configuration context to help identify the content in the configuration file. The no form of this command removes the string from the configuration.
Default	No description associated with the configuration context.
Parameters	<i>string</i> — 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.

System Information Commands

boot-bad-exec

Syntax	boot-bad-exec <i>file-url</i> no boot-bad-exec																					
Context	config>system																					
Description	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. The commands are persistent between router (re)boots and are included in the configuration saves (admin>save).																					
Default	no boot-bad-exec																					
Parameters	<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. <table><tr><td>Values</td><td>file url:</td><td>local-url remote-url: 255 chars max</td></tr><tr><td></td><td>local-url:</td><td>[<cflash-id/> <usb-flash-id>][file-path]</td></tr><tr><td></td><td>remote-url:</td><td>[{ftp://} login:pswd@remote-locn/][file-path]</td></tr><tr><td></td><td></td><td>remote-locn [<i>hostname</i> <i>ipv4-address</i>]</td></tr><tr><td></td><td>ipv4-address</td><td>a.b.c.d</td></tr><tr><td></td><td>cflash-id:</td><td>cf1:</td></tr><tr><td></td><td>usb-flash-id</td><td>uf1:</td></tr></table>	Values	file url:	local-url remote-url: 255 chars max		local-url:	[<cflash-id/> <usb-flash-id>][file-path]		remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]			remote-locn [<i>hostname</i> <i>ipv4-address</i>]		ipv4-address	a.b.c.d		cflash-id:	cf1:		usb-flash-id	uf1:
Values	file url:	local-url remote-url: 255 chars max																				
	local-url:	[<cflash-id/> <usb-flash-id>][file-path]																				
	remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]																				
		remote-locn [<i>hostname</i> <i>ipv4-address</i>]																				
	ipv4-address	a.b.c.d																				
	cflash-id:	cf1:																				
	usb-flash-id	uf1:																				
Related Commands	exec command on page 51 — This command executes the contents of a text file as if they were CLI commands entered at the console.																					

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.
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.

Values	file url:	local-url remote-url: 255 chars max
	local-url:	[<cf-flash-id/> <usb-flash-id>][file-path]
	remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]
		remote-locn [<i>hostname</i> <i>ipv4-address</i>]
	ipv4-address	a.b.c.d
	cf-flash-id:	cf1:
	usb-flash-id	uf1:

Related Commands **exec command on page 51** — This command executes the contents of a text file as if they were CLI commands entered at the console.

cli-code

Syntax	cli-code <i>cli-code</i> no cli-code
Context	config>system
Description	This command creates a Common Language Location Identifier (CLLI) code string for the 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	<i>cli-code</i> — 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 <i>count</i> no config-backup
Context	config>system
Description	This command configures the maximum number of backup versions maintained for configuration files and BOF. 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.

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 is performed for all configurations and their associated persistent index files.

The **no** form of the command returns the configuration to the default value.

Default 5

Parameters *count* — The maximum number of backup revisions.

Values 1 — 9

contact

Syntax **contact** *contact-name*
no contact

Context config>system

Description This command creates a text string that identifies the contact name for the device.
 Only one contact can be configured, if multiple contacts are configured the last one entered will overwrite the previous entry.

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

Default none — No contact name is configured.

Parameters *contact-name* — 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.

coordinates

Syntax **coordinates** *coordinates*
no coordinates

Context config>system

Description This command creates a text string that identifies the system coordinates for the device location. For example, the command **coordinates** "37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.

Only one set of coordinates can be configured. If multiple coordinates are configured, the last one entered overwrites the previous entry.

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

Default none — No coordinates are configured.

Parameters *coordinates* — 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.

lacp-system-priority

Syntax **lacp-system-priority** *lacp-system-priority*
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 32768

Parameters *lacp-system-priority* — Specifies the LACP system priority.

Values 1 — 65535

location

Syntax **location** *location*
no location

Context config>system

Description This command creates a text string that identifies the system location for the device.
Only one location can be configured. If multiple locations are configured, the last one entered overwrites the previous entry.

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

Default **none** — No system location is configured.

Parameters *location* — 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.

login-control

Syntax	<i>login-control</i>
Context	config>system
Description	This command enables the context to configure login control.

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. <pre>ABC>config>system# name "ALA-1" ALA-1>config>system#</pre> 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.

power-supply

Syntax	power-supply [<i>power-supply-id</i>] <i>type</i>
Context	config>system
Description	This command enables the context to configure a power-supply. On 7210 SAS-D ETR, by default, the software does not generate any traps or alarms for PS2, when the external power- supply failure has been detected. The user is provided with an option to configure the external backup power-supply type. Only if the user configures the power-supply type as 'ac' or 'dc' the system generates alarm or trap on a power-supply failure. The user can disable generation of alarms or traps by setting the value to 'none'. NOTES:

1. By setting the value to 'none', the software does not send out a trap to the management station to clear the alarm, if there was one pending. The 'none' value only clears the trap locally and resets the LED color, if there are no other major or critical alarms pending. It is expected that the management station takes appropriate action on receiving the configuration change event or trap.
2. This CLI command does not affect generation of trap or alarm for the integrated power supply. Traps or alarms are always generated on detection of failure of the integrated power supply, when an external power supply is in use.
3. The 7210 SAS-D ETR does not have the capability to detect the power-supply type, that is, it cannot detect if the external power-supply type is an AC or DC version. Therefore, the user configured value is not validated by the software. It is the users responsibility to ensure if it is correct and corresponds to what they are using. If they provide a wrong value, the software continues to display the configured value and generate traps or alarms.
4. The 'power-supply' command is applicable only to 7210 SAS-D ETR. If used on 7210 SAS-D, the software returns an error message.

Parameters *power-supply-id* — Identifies the power-supply for which the 'type' is to be applied.

Values 2 - Identifies the optional external backup power supply on the 7210 SAS-D ETR.

type — Identifies the type of power-supply.

Values keywords - dc|ac|none

vwm-shelf

Syntax **[no] vwm-shelf vwm-shelf-id [create]**

Context config>system

Description Provides the context to configure the shelf information for 1830 VWM clip-on device.

The user must create the VWM clip-on device and provision the shelf ID to allow the 7210 software to communicate with the shelf and retrieve information. The value specified in the parameter vwm-shelf-id must match the shelf ID set using the rotary dial on the clip-on device. If these shelf IDs do not match, 7210 SAS devices cannot communicate to the device and will not provide any information about the device. 7210 software cannot detect a mismatch between the value of the configured vwm-shelf-id and the shelf ID set on the rotary dial. 7210 SAS software raises an event/log to alert user about possible mismatch in configuration of shelf IDs.

The software allows user to configure only a single clip-on device for management by specifying a single shelf ID. Software will not allow for configuration of more than a single clip-on shelf.

The no form of the command removes the configured shelf ID and the software forgets all the information it has for the shelf.

Default No default value is used.

Parameters *vwm-shelf-id* — The Shelf ID used to identify the 1830 VWM clip-on device attached to 7210.

Values 1-7

shutdown

Syntax	[no] shutdown
Context	config> system> vwm-shelf <vwm-shelf-id>
Description	This CLI command allows the user to administratively disable the management of the clip-on device identified by the parameter <i>vwm-shelf-id</i>. When this command is executed, 7210 software will clear all pending events/traps/alarms related to this shelf. The no form of the command allows the user to administratively enable the management of the clip-on device. The software raises appropriate events/traps/alarms for the device.
Default	no shutdown

System Alarm Commands

alarm

Syntax	alarm <i>rmon-alarm-id</i> variable-oid <i>oid-string</i> interval <i>seconds</i> [<i>sample-type</i>] [startup-alarm <i>alarm-type</i>] [rising-event <i>rmon-event-id</i> rising-threshold <i>threshold</i>] [falling-event <i>rmon-event-id</i> falling-threshold <i>threshold</i>] [owner <i>owner-string</i>] no alarm <i>rmon-alarm-id</i>
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.
Parameters	<i>rmon-alarm-id</i> — The rmon-alarm-id is a numerical identifier for the alarm being configured. The number of alarms that can be created is limited to 1200. Default None Values 1 — 65535 variable-oid <i>oid-string</i> — The oid-string is the SNMP object identifier of the particular variable to be sampled. Only SNMP variables that resolve to an ASN.1 primitive type of integer (integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. The oid-string may be expressed using either the dotted string notation or as object name plus dotted instance identifier. For example, "1.3.6.1.2.1.2.2.1.10.184582144" or "ifInOctets.184582144". The oid-string has a maximum length of 255 characters Default None interval <i>seconds</i> — The interval in seconds specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. When setting this interval value, care should be taken in the case of 'delta' type sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2147483647 - 1 during a single sampling interval. Care should also be taken not to set the interval value too low to avoid creating unnecessary processing overhead. Default None Values 1 — 2147483647

sample-type — Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds.

Default **Absolute**

Values **absolute** — Specifies that the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval.
delta — Specifies that the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

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**

rising-event rmon-event-id — The identifier of the 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' is configured, the CLI requires a 'rising-threshold' to also be configured.

Default 0

Values 0 — 65535

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.

Default 0

Values -2147483648 — 2147483647

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.

Default 0

Values -2147483648 — 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 rising 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** *threshold* value.

Default 0

Values -2147483648 — 2147483647

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"
```

cflash-cap-alarm

Syntax **cflash-cap-alarm** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*]
interval *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-alarm *cflash-id*

Context config>system>thresholds

Description This command enables capacity monitoring of the compact flash specified in this command. The severity level is alarm. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold alarm.

Parameters *cflash-id* — The cflash-id specifies the name of the cflash device to be monitored.

Values cfl:, cfl-A:

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.

Default 0

Values -2147483648 — 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 rising threshold crossing event is generated, another such event will not be generated until the sampled value raises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* — Specifies the polling period, in seconds, over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 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 a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

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.

Default either

Values rising, falling, 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-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	This command enables capacity monitoring of the compact flash specified in this command. The severity level is warning. Both a rising and falling threshold can be specified. The no form of this command removes the configured compact flash threshold warning.
Parameters	<i>cflash-id</i> — The cflash-id specifies the name of the cflash device to be monitored. Values cfl:, cfl-A: 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. Default 0 Values -2147483648 — 2147483647 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. After a rising threshold crossing event is generated, another such event will not be generated until the sampled value raises above this threshold and reaches greater than or equal the rising-threshold value. Default 0 Values -2147483648 — 2147483647 interval <i>seconds</i> — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. Values 1 — 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.

trap — In the case of 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 — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of 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:

```
cflash-cap-warn cfl-B: rising-threshold 2000000 falling-threshold 1999900 interval 240 rmon-
event-type trap start-alarm either
```

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.

Parameters **rmon-event-type** — The 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.

trap — In the case of 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 — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of 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 *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:

Default event 5 rmon-event-type both description "alarm testing" owner "TiMOS CLI"

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 <code>sgiMemoryUsed</code> 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.
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. Default 0 Values -2147483648 — 2147483647 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. After a rising threshold crossing event is generated, another such event will not be generated until the sampled value raises above this threshold and reaches greater than or equal the rising-threshold threshold value. Default 0 Values -2147483648 — 2147483647 interval <i>seconds</i> — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. Values 1 — 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 an OS logger entry. The RMON-MIB log table entries can be viewed using the CLI command. trap — In the case of 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 — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of 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 <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-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.
Parameters	rising-threshold <i>threshold</i> — The rising-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. Default 0 Values -2147483648 — 2147483647

falling-threshold *threshold* — The falling-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 rising threshold crossing event is generated, another such event will not be generated until the sampled value raises above this threshold and reaches greater than or equal the rising-threshold threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* — The interval in seconds specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 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.

trap — In the case of 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 — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

Values log, trap, both, none

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.

thresholds

Syntax	thresholds
Context	config>system
Description	This command enables the context to configure monitoring thresholds.

PTP Commands

ptp

Syntax	[no] ptp
Context	config>system
Description	This command enables the context to configure parameters for IEEE 1588-2008, Precision Time Protocol. This command is only available on the control assemblies that support 1588.

shutdown

Syntax	[no] shutdown
Context	config>system>ptp
Description	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 to do a 'no shutdown' on hardware that does not support PTP, an alarm will be raised to indicate limited capabilities. When ptp is shutdown, the PTP slave port is not operational. It shall not be considered as a source for system timing.
Default	shutdown

clock-type

Syntax	clock-type {{ordinary [slave]}}
Context	config>system>ptp
Description	This command configures the type of clock. The clock-type can only be changed when ptp is shutdown. The clock-type cannot be changed to master-only if PTP reference is no shutdown. In addition, clock-type cannot be changed to master-only if there are peers configured.
Default	ordinary slave
Parameters	<i>ordinary</i> — The clock is capable of being either a PTP grandmaster or slave. <i>slave</i> — The clock supports boundary-clock functionality (master and slave concurrently).

domain

Syntax	[no] domain <i>domain</i>
Context	config>system>ptp
Description	This command configures the PTP domain. The no form of the command reverts to the default configuration. 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. 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.
Default	0 for ieee1588-2008 or 4 for g8265dot1-2010
Parameters	<i>domain</i> — The PTP domain.
Values	0-255

log-sync-interval

Syntax	[no] log-sync-interval <i>value</i>
Context	config>system>ptp
Description	This command allows the user to configure the PTP Sync and PTP Delay-Req message rate that a PTP slave requests of a PTP master. The value specified is used as the rate for both PTP Sync and Delay-Req messages. User can set a lower pps rate, typically when using syncE for frequency and PTP for only time. The no form of the command sets it to a default value of 64pps.
Default	64pps
Parameters	<i>value</i> — Specifies the rate for both PTP Sync and Delay-Req messages.
Values	-6, -5, -4, and -3

Table 24: Values and the corresponding pps rate

Value	pps Rate
-6	64pps
-5	32pps
-4	16pps
-3	8pps

priority1

Syntax	[no] priority1 <i>priority</i>
Context	config>system>ptp 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. Note: This value is used both 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. The no form of the command reverts to the default configuration.
Default	128
Parameters	<i>priority</i> — Specifies the value of the priority1 field. Values 0-255

priority2

Syntax	[no] priority2 <i>priority</i>
Context	config>system>ptp
	This command configures the priority2 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.
	Note: This value is used both 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	128
Parameters	<i>priority</i> — Specifies the value of the priority2 field.
	Values 0-255

profile

Syntax	profile { ieee1588-2008 g8265dot1-2010 }
Context	config>system>ptp
Description	This command configures the profile to be used for the internal ptp clock. This principally defines the BMCA behaviour.
	The profile cannot be changed unless ptp is shutdown.
	When the profile is changed, the domain is changed to the default value for the new profile. In addition, if the profile is changed to ieee1588-2008, the wait-to-retorestore timer is disabled.
Default	ieee1588-2008
Parameters	ieee1588-2008 — Conform to the default BMCA of the 2008 version of the IEEE1588 standard.
	g.8265.1-2010 — Conform to the BMCA specified in the ITU-T G.8265.1 specification.

network-type

Syntax	network-type <sonet sdh>
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 7750 will support the reception of any valid value in Table 1/G.8265.1

PTP Commands

Default	sdh
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>
Context	config>system>ptp This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer. Up to twenty 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 & enabled. Peers cannot be created when the clock-type is ordinary master.
Default	none
Parameters	<i>ip-address</i> — The IP address of the remote peer. Values ipv4-address a.b.c.d

priority

Syntax	priority <i>local_priority</i>
Context	configure>system>ptp>peer> This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is only relevant when the g.8265.1-2010 profile is selected. The parameter is ignored when the ieee1588-2008 profile is selected. 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. There is a limit of 20 configured PTP peers.
Default	128
Parameters	<i>local_priority</i> — Specifies the value of the local priority. Values 1-255

shutdown

Syntax [no] shutdown

Context configure>system>ptp>peer

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.

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

Default no shutdown

Date and Time Commands

set-time

Syntax	set-time [<i>date</i>] [<i>time</i>]						
Context	admin						
Description	This command sets the local system time. The time entered should be accurate for the time zone configured for the system. The system 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.						
Parameters	<i>date</i> — The local date and time accurate to the minute in the YYYY/MM/DD format. <table><tr><td>Values</td><td><i>YYYY</i> is the four-digit year <i>MM</i> is the two-digit month <i>DD</i> is the two-digit date</td></tr></table> <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. <table><tr><td>Default</td><td>0</td></tr><tr><td>Values</td><td><i>hh</i> is the two-digit hour in 24 hour format (00=midnight, 12=noon) <i>mm</i> is the two-digit minute</td></tr></table>	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	Default	0	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
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						
Default	0						
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						

time

Syntax	time
Context	config>system
Description	This command enables the context to configure the system time zone and time synchronization parameters.

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	none

authentication-check

Syntax	[no] authentication-check
Context	config>system>time>ntp
Description	This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type or key. When authentication-check is 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. The no form of this command allows authentication mismatches to be accepted; the counters however are maintained.
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	none
Parameters	<i>key-id</i> — Configure the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets. Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry. 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. Default None Values 1 — 255 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. The key can be any combination of ASCII characters up to maximum 8 characters in length for message-digest (md5) or maximum 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 (“ ”). 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 a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified. hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, this means that hash2 encrypted variable can't be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified. type — This parameter determines if DES or message-digest authentication is used. This is a required parameter; either DES or message-digest must be configured. Values des — Specifies that DES authentication is used for this key message-digest — Specifies that MD5 authentication in accordance with RFC 2104 is used for this key.

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	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. The no form of this command removes the address from the configuration.
Parameters	<i>router</i> — Specifies the router name used to transmit NTP packets. Base is the default and the only router name supported currently. Values Base Default Base <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. Values 32 character maximum 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. Values 1 — 255 Default none 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. Values 2 — 4 Default 4 ttl <i>ttl</i> — Specifies the IP Time To Live (TTL) value. Values 1 — 255 Default none

broadcastclient

Syntax	broadcastclient [router <i>router-name</i>] {interface <i>ip-int-name</i> } [authenticate] no broadcastclient [router <i>router-name</i>] {interface <i>ip-int-name</i> }
Context	config>system>time>ntp
Description	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. The no form of this command removes the address from the configuration.
Parameters	router <i>router-name</i> — Specifies the router name used to receive NTP packets. Values Base Default Base interface <i>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. Values 32 character maximum authenticate — Specifies whether or not to require authentication of NTP PDUs. When enabled, NTP PDUs are authenticated upon receipt.

ntp-server

Syntax	ntp-server [transmit <i>key-id</i>] no ntp-server
Context	config>system>time>ntp
Description	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.
Default	no ntp-server
Parameters	<i>key-id</i> — If specified, requires client packets to be authenticated. Values 1 — 255 Default None

peer

Syntax	peer <i>ip-address</i> [key-id <i>key-id</i>] [version <i>version</i>] [prefer] no peer <i>ip-address</i>
Context	config>system>time>ntp
Description	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. The no form of the command removes the configured peer.
Parameters	<i>ip-address</i> — Configure the IP address of the peer that requires a peering relationship to be set up. This is a required parameter. Default None Values Any valid IP-address key-id <i>key-id</i> — Successful authentication requires that both peers must have configured the same authentication key-id, type and key value. 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. Default None Values 1 — 255 version <i>version</i> — Specify 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. Default 4 Values 2 — 4 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.

server

Syntax	server <i>ip address</i> [key-id <i>key-id</i>] [version <i>version</i>] [prefer] no server <i>ip address</i>
Context	config>system>time>ntp
Description	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. Up to five NTP servers can be configured.
Parameters	<i>ip-address</i> — Configure the IP address of a node that acts as an NTP server to this network element. This is a required parameter. Values Any valid IP address key-id <i>key-id</i> — Enter 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. Values 1 — 255 version <i>version</i> — Use this command to configure the NTP version number that is expected by this node. This is an optional parameter Default 4 Values 2 — 4 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.

SNTP Commands

sntp

Syntax	[no] sntp
Context	config>system>time
Description	This command creates the context to edit the Simple Network Time Protocol (SNTP). SNTP can be configured in either broadcast or unicast client mode. SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from SNTP/NTP servers. It cannot be used to provide time services to other systems. The system clock is adjusted automatically during system initialization and periodically to ensure that the local time is close to server's time. However, if the time difference between the SNTP/NTP server and the system clock is more than 2.5 seconds, the software corrects the system time gradually adjusted over an interval. SNTP is created in an administratively enabled state (no shutdown). The no form of the command removes the SNTP instance and configuration. SNTP does not need to be administratively disabled when removing the SNTP instance and configuration.
Default	no sntp

broadcast-client

Syntax	[no] broadcast-client
Context	config>system>time>sntp
Description	This command enables listening to SNTP/NTP broadcast messages on interfaces with broadcast client enabled at global device level. SNTP must be shutdown prior to changing either to or from broadcast mode. The no form of the command disables broadcast client mode.
Default	no broadcast-client

server-address

Syntax	server-address <i>ip-address</i> [version <i>version-number</i>] [normal preferred] [interval <i>seconds</i>] no server-address										
Context	config>system>time>sntp										
Description	This command creates an SNTP server for unicast client mode.										
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. <table><tr><td>Values</td><td>1 — 3</td></tr><tr><td>Default</td><td>3</td></tr></table> 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. <table><tr><td>Default</td><td>normal</td></tr></table> interval <i>seconds</i> — Specifies the frequency at which this server is queried. <table><tr><td>Values</td><td>64 — 1024</td></tr><tr><td>Default</td><td>64</td></tr></table>	Values	1 — 3	Default	3	Default	normal	Values	64 — 1024	Default	64
Values	1 — 3										
Default	3										
Default	normal										
Values	64 — 1024										
Default	64										

CRON Commands

cron

Syntax	cron
Context	config
Description	This command creates the context to create scripts, script parameters and schedules which support the Service Assurance Agent (SAA) functions. 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.

action

Syntax	[no] action <i>action-name</i> [owner <i>action-owner</i>]
Context	config>cron config>cron>sched
Description	This command configures action parameters for a script.
Default	none
Parameters	action <i>action-name</i> — Specifies the action name. Values Maximum 32 characters. owner <i>action-owner</i> — Specifies the owner name. Default TiMOS CLI

expire-time

Syntax	expire-time {seconds forever}
Context	config>cron>action
Description	This command configures the maximum amount of time to keep the results from a script run.
Parameters	seconds — Specifies the maximum amount of time to keep the results from a script run. Values 1 — 21474836 Default 3600 (1 hour) forever — Specifies to keep the results from a script run forever.

lifetime

Syntax	lifetime {seconds forever}
Context	config>cron>action
Description	This command configures the maximum amount of time the script may run.
Parameters	seconds — Specifies the maximum amount of time to keep the results from a script run. Values 1 — 21474836 Default 3600 (1 hour) forever — Specifies to keep the results from a script run forever.

max-completed

Syntax	max-completed <i>unsigned</i>
Context	config>cron>action
Description	This command specifies the maximum number of completed sessions to keep in the event execution log. If a new event execution record exceeds the number of records specified this command, the oldest record is deleted. The no form of this command resets the value to the default.
Parameters	<i>unsigned</i> — Specifies the maximum number of completed sessions to keep in the event execution log. Values 0 — 255 Default 1

results

Syntax	[no] results <i>file-url</i>
Context	config>cron>action
Description	This command specifies the location where the system writes the output of an event script's execution. The no form of this command removes the file location from the configuration.
Parameters	<i>file-url</i> — Specifies the location where the system writes the output of an event script's execution. Values file url: local-url remote-url: 255 chars max local-url: [<cf-flash-id>/ <usb-flash-id>/][<file-path>] remote-url: [{ftp://} login:pswd@remote-locn/][file-path] remote-locn [hostname ipv4-address] ipv4-address a.b.c.d


```

cflash-id:    cfl:
usb-flash-id  ufl:

```

script

Syntax	[no] script <i>script-name</i> [owner <i>owner-name</i>]
Context	config>cron>action
Description	This command creates action parameters for a script including the maximum amount of time to keep the results from a script run, the maximum amount of time a script may run, the maximum number of script runs to store and the location to store the results. The no form of this command removes the script parameters from the configuration.
Default	none — No server-address is configured.
Parameters	script <i>script-name</i> — The script command in the action context connects and event to the script which will run when the event is triggered. owner <i>owner-name</i> — Owner name of the schedule. Default TiMOS CLI The no form of this command removes the script entry from the action context.

schedule

Syntax	[no] schedule <i>schedule-name</i> [owner <i>owner-name</i>]
Context	config>cron
Description	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). The no form of the command removes the context from the configuration.
Default	none
Parameters	<i>schedule-name</i> — Name of the schedule. owner <i>owner-name</i> — Owner name of the schedule.

count

Syntax	count <i>number</i>
Context	config>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.
Parameters	<i>number</i> — The number of times the schedule is run.
Values	1 — 65535
Default	65535

day-of-month

Syntax	[no] day-of-month { <i>day-number</i> [<i>..day-number</i>] all }
Context	config>cron>sched
Description	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. 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). The no form of this command removes the specified day-of-month from the list.
Parameters	<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. Integer values must map to a valid day for the month in question. For example, February 30 is not a valid date. Values 1 — 31, -31 — -1 (maximum 62 day-numbers) all — Specifies all days of the month.

end-time

Syntax	[no] end-time [<i>date</i> <i>day-name</i>] <i>time</i>
Context	config>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.

Parameters	<i>date</i> — Specifies the date to schedule a command.
	Values YYYY:MM:DD in year:month:day number format
	<i>day-name</i> — Specifies the day of the week to schedule a command.
	Values sunday monday tuesday wednesday thursday friday saturday
	<i>time</i> — Specifies the time of day to schedule a command.
	Values hh:mm in hour:minute format

hour

Syntax	[no] hour {.. <i>hour-number</i> [.. <i>hour-number</i>] all }
Context	config>cron>sched
Description	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. The no form of this command removes the specified hour from the configuration.
Parameters	<i>hour-number</i> — Specifies the hour to schedule a command. Values 0 — 23 (maximum 24 hour-numbers) all — Specifies all hours.

interval

Syntax	[no] interval <i>seconds</i>
Context	config>cron>sched
Description	This command specifies the interval between runs of an event.
Parameters	<i>seconds</i> — The interval, in seconds, between runs of an event. Values 30 — 4,294,967,295

minute

Syntax	[no] minute { <i>minute-number</i> [<i>..minute-number</i>] all }
Context	config>cron>sched
Description	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. The no form of this command removes the specified minute from the configuration.
Parameters	<i>minute-number</i> — Specifies the minute to schedule a command. Values 0 — 59 (maximum 60 minute-numbers) all — Specifies all minutes.

month

Syntax	[no] month { <i>month-number</i> [<i>..month-number</i>] <i>month-name</i> [<i>..month-name</i>] all }
Context	config>cron>sched
Description	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. The no form of this command removes the specified month from the configuration.
Parameters	month-number — Specifies a month number. Values 1 —12 (maximum 12 month-numbers) all — Specifies all months. month-name — Specifies a month by name Values january, february, march, april, may, june, july, august, september, october, november, december (maximum 12 month names)

type

Syntax	type { <i>schedule-type</i> }
Context	config>cron>sched
Description	This command specifies how the system should interpret the commands contained within the schedule node.
Parameters	<i>schedule-type</i> — Specify the type of schedule for the system to interpret the commands contained within the schedule node.

Values	periodic — Specifies a schedule which runs at a given interval. interval must be specified for this feature to run successfully. 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. oneshot — Specifies a schedule which runs one time only. 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	[no] weekday { <i>weekday-number</i> [<i>..weekday-number</i>] <i>day-name</i> [<i>..day-name</i>] all }
Context	config>cron>sched
Description	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. 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). The no form of this command removes the specified weekday from the configuration.
Parameters	day-number — Specifies a weekday number. Values 1 —7 (maximum 7 week-day-numbers) day-name — Specifies a day by name Values sunday, monday, tuesday, wednesday, thursday, friday, saturday (maximum 7 week-day names) all — Specifies all days of the week.

script

Syntax	[no] script <i>script-name</i> [owner <i>owner-name</i>]
Context	config>cron>script
Description	This command configures the name associated with this script.
Parameters	<i>script-name</i> — Specifies the script name.

location

Syntax	[no] location <i>file-url</i>		
Context	config>cron>script		
Description	This command configures the location of script to be scheduled.		
Parameters	<i>file-url</i> — Specifies the location where the system writes the output of an event script’s execution.		
	Values	file url:	local-url remote-url: 255 chars max
		local-url:	[<cflash-id>/ <usb-flash-id>/][<file-path>]
		remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]
			remote-locn [<i>hostname</i> <i>ipv4-address</i>]
			ipv4-address a.b.c.d
		cflash-id:	cfl:
		usb-flash-id	ufl:

Time Range Commands

time-range

Syntax	[no] time-range <i>name</i> [create]
Context	config>cron
Description	This command configures a time range. The no form of the command removes the <i>name</i> from the configuration.
Default	none
Parameters	<i>name</i> — Configures a name for the time range up to 32 characters in length.

absolute

Syntax	absolute start <i>start-absolute-time</i> end <i>end-absolute-time</i> no absolute start <i>absolute-time</i>																								
Context	config>cron>time-range																								
Description	This command configures an absolute time interval that will not repeat. The no form of the command removes the absolute time range from the configuration.																								
Parameters	start <i>absolute-time</i> — Specifies starting parameters for the absolute time-range. <table> <tr> <td>Values</td><td>absolute-time: year/month/day, hh:mm</td></tr> <tr> <td></td><td>year: 2005 — 2099</td></tr> <tr> <td></td><td>month: 1 — 12</td></tr> <tr> <td></td><td>day: 1 — 31</td></tr> <tr> <td></td><td>hh: 0 — 23</td></tr> <tr> <td></td><td>mm: [0 — 59</td></tr> </table> end <i>absolute-time</i> — Specifies end parameters for the absolute time-range. <table> <tr> <td>Values</td><td>absolute-time: year/month/day, hh:mm</td></tr> <tr> <td></td><td>year: 2005 — 2099</td></tr> <tr> <td></td><td>month: 1 — 12</td></tr> <tr> <td></td><td>day: 1 — 31</td></tr> <tr> <td></td><td>hh: 0 — 23</td></tr> <tr> <td></td><td>mm: [0 — 59</td></tr> </table>	Values	absolute-time: year/month/day, hh:mm		year: 2005 — 2099		month: 1 — 12		day: 1 — 31		hh: 0 — 23		mm: [0 — 59	Values	absolute-time: year/month/day, hh:mm		year: 2005 — 2099		month: 1 — 12		day: 1 — 31		hh: 0 — 23		mm: [0 — 59
Values	absolute-time: year/month/day, hh:mm																								
	year: 2005 — 2099																								
	month: 1 — 12																								
	day: 1 — 31																								
	hh: 0 — 23																								
	mm: [0 — 59																								
Values	absolute-time: year/month/day, hh:mm																								
	year: 2005 — 2099																								
	month: 1 — 12																								
	day: 1 — 31																								
	hh: 0 — 23																								
	mm: [0 — 59																								

daily

Syntax	daily start <i>start-time-of-day</i> end <i>end-time-of-day</i> no daily start <i>start-time-of-day</i>																		
Context	config>cron>time-range																		
Description	This command configures the start and end of a schedule for every day of the week. To configure a daily time-range across midnight, use a combination of two entries. An entry that starts at hour zero will take over from an entry that ends at hour 24. The no form of the command removes the daily time parameters from the configuration.																		
Parameters	<i>start-time-of-day</i> — Specifies the starting time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 23</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table> <i>end-time-of-day</i> — Specifies the ending time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 24</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table>	Values	Syntax:	hh:mm		hh	0 — 23		mm	0 — 59	Values	Syntax:	hh:mm		hh	0 — 24		mm	0 — 59
Values	Syntax:	hh:mm																	
	hh	0 — 23																	
	mm	0 — 59																	
Values	Syntax:	hh:mm																	
	hh	0 — 24																	
	mm	0 — 59																	

weekdays

Syntax	weekdays start <i>start-time-of-day</i> end <i>end-time-of-day</i> no weekdays start <i>start-time-of-day</i>																		
Context	config>cron>time-range																		
Description	This command configures the start and end of a weekday schedule. The no form of the command removes the weekday parameters from the configuration.																		
Parameters	<i>start-time-of-day</i> — Specifies the starting time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 23</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table> <i>end-time-of-day</i> — Specifies the ending time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 24</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table>	Values	Syntax:	hh:mm		hh	0 — 23		mm	0 — 59	Values	Syntax:	hh:mm		hh	0 — 24		mm	0 — 59
Values	Syntax:	hh:mm																	
	hh	0 — 23																	
	mm	0 — 59																	
Values	Syntax:	hh:mm																	
	hh	0 — 24																	
	mm	0 — 59																	

weekend

Syntax	weekend start <i>start-time-of-day</i> end <i>end-time-of-day</i> no weekend start <i>start-time-of-day</i>																		
Context	config>cron>time-range																		
Description	This command configures a time interval for every weekend day in the time range. The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. An 11:00 start and end time is invalid. This example configures a start at 11:00 and an end at 11:01 on both Saturday and Sunday. The no form of the command removes the weekend parameters from the configuration.																		
Parameters	<i>start-time-of-day</i> — Specifies the starting time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 23</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table> <i>end-time-of-day</i> — Specifies the ending time for the time range. <table><tr><td>Values</td><td>Syntax:</td><td>hh:mm</td></tr><tr><td></td><td>hh</td><td>0 — 24</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table>	Values	Syntax:	hh:mm		hh	0 — 23		mm	0 — 59	Values	Syntax:	hh:mm		hh	0 — 24		mm	0 — 59
Values	Syntax:	hh:mm																	
	hh	0 — 23																	
	mm	0 — 59																	
Values	Syntax:	hh:mm																	
	hh	0 — 24																	
	mm	0 — 59																	

weekly

Syntax	weekly start <i>start-time-in-week</i> end <i>end-time-in-week</i> no weekly start <i>start-time-in-week</i>																		
Context	config>cron>time-range																		
Description	This command configures a weekly periodic interval in the time range. The no form of the command removes the weekly parameters from the configuration.																		
Parameters	<i>start-time-in-week</i> — Specifies the start day and time of the week. <table><tr><td>Values</td><td>Syntax:</td><td>day, hh:mm</td></tr><tr><td></td><td>day</td><td>sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday</td></tr><tr><td></td><td>hh</td><td>0 — 23</td></tr><tr><td></td><td>mm</td><td>0 — 59</td></tr></table> <i>end-time-in-week</i> — Specifies the end day and time of the week. <table><tr><td>Values</td><td>Syntax:</td><td>day, hh:mm</td></tr><tr><td>Values</td><td>day</td><td>sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday</td></tr></table>	Values	Syntax:	day, hh:mm		day	sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday		hh	0 — 23		mm	0 — 59	Values	Syntax:	day, hh:mm	Values	day	sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday
Values	Syntax:	day, hh:mm																	
	day	sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday																	
	hh	0 — 23																	
	mm	0 — 59																	
Values	Syntax:	day, hh:mm																	
Values	day	sun, mon, tue, wed, thu, fri, sat sunday, monday, tuesday, wednesday, thursday, friday, saturday																	

hh 0 — 24
mm 0 — 59

weekly start *time-in-week* **end** *time-in-week* — This parameter configures the start and end of a schedule for the same day every week, for example, every Friday. The start and end dates must be the same. The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. A start time and end time of 11:00 is invalid.

Values 00 — 23, 00 — 59

Default no time-range

Time of Day Commands

tod-suite

Syntax	[no] tod-suite <i>tod-suite name</i> create
Context	config>cron
Description	This command creates the tod-suite context.
Default	no tod-suite

egress

Syntax	egress
Context	config>cron>tod-suite
Description	This command enables the TOD suite egress parameters.

ingress

Syntax	ingress
Context	config>cron>tod-suite
Description	This command enables the TOD suite ingress parameters.

filter

Syntax	filter ip <i>ip-filter-id</i> [time-range <i>time-range-name</i>] [priority <i>priority</i>] filter mac <i>mac-filter-id</i> [time-range <i>time-range-name</i>] [priority <i>priority</i>] no ip <i>ip-filter-id</i> [time-range <i>time-range-name</i>] no filter mac <i>mac-filter-id</i> [time-range <i>time-range-name</i>]
Context	config>cron>tod-suite>egress config>cron>tod-suite>ingress
Description	This command creates time-range based associations of previously created filter policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range.
Parameters	ip-filter <i>ip-filter-id</i> — Specifies an IP filter for this tod-suite.

Values 1 — 65535

time-range *time-range-name* — Name for the specified time-range. If the time-range is not populated the system will assume the assignment to mean “all times”. Only one entry without a time-range is allowed for every type of policy. The system does not allow the user to specify more than one policy with the same time-range and priority.

Values Up to 32 characters

priority *priority* — Priority of the time-range. Only one time-range assignment of the same type and priority is allowed.

Values 1 — 10

mac *mac-filter-id* — Specifies a MAC filter for this tod-suite.

Values 1 — 65535

qos

Syntax **qos** *policy-id* [**time-range** *time-range-name*] [**priority** *priority*]
no qos *policy-id* [**time-range** *time-range-name*] [

Context config>cron>tod-suite>ingress

Description This command creates time-range based associations of previously created QoS policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range.

The no form of the command reverts to the

Parameters **policy-id** — Specifies an egress QoS policy for this tod-suite.

Values 1 — 65535

time-range *time-range-name* — Name for the specified time-range. If the time-range is not populated the system will assume the assignment to mean “all times”. Only one entry without a time-range is allowed for every type of policy. The system does not allow the user to specify more than one policy with the same time-range and priority.

Values Up to 32 characters

Default "NO-TIME-RANGE" policy

priority *priority* — Priority of the time-range. Only one time-range assignment of the same type and priority is allowed.

Values 1 — 10

Default 5

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	This command configures the start and end dates and offset for summer time or daylight savings time to override system defaults or for user defined time zones. When configured, the time is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends. If the time zone configured is listed in Table 17, System-defined Time Zones, on page 177, 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 17 or entered as optional parameters in this command. Up to five summer time zones may be configured, for example, for five successive years or for five different time zones. Configuring a sixth entry 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	<i>std-zone-name</i> — The standard time zone name. The standard name must be a system-defined zone in Table 17. 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, NDT, NZDT <i>non-std-zone-name</i> — The non-standard time zone name. Create a user-defined name created using the zone command on page 327 Values 5 characters maximum

end

Syntax	end { <i>end-week</i> } { <i>end-day</i> } { <i>end-month</i> } [<i>hours-minutes</i>]
Context	config>system>time>dst-zone
Description	This command configures start of summer time settings.
Parameters	<i>end-week</i> — Specifies the starting week of the month when the summer time will end. Values first, second, third, fourth, last Default first <i>end-day</i> — Specifies the starting day of the week when the summer time will end. Values sunday, monday, tuesday, wednesday, thursday, friday, saturday Default sunday <i>end-month</i> — 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 <i>hours</i> — Specifies the hour at which the summer time will end. Values 0 — 24 Default 0 <i>minutes</i> — Specifies the number of minutes, after the hours defined by the <i>hours</i> parameter, when the summer time will end. Values 0 — 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.
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. Default 60

Values 0 — 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.
Parameters	start-week — 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. Default sunday Values sunday, monday, tuesday, wednesday, thursday, friday, saturday 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 <i>hours</i> parameter, when the summer time will take effect. Default 0

zone

Syntax	zone [<i>std-zone-name</i> <i>non-std-zone-name</i>] [<i>hh</i> [: <i>mm</i>]] no zone
Context	config>system>time
Description	This command sets the time zone and/or time zone offset for the device. The OS supports system-defined and user-defined time zones. The system-defined time zones are listed in Table 17, System-defined Time Zones, on page 177. 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 17](#). 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.

Default hours: 0
 minutes: 0

Values hours: -11 — 12
 minutes: 0 — 59

System Synchronization 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 (The ref-order must be specified in order for this command to be enabled.)

abort

Syntax	abort
Context	config>system>sync-if-timing
Description	This command is required to discard changes that have been made to the synchronous interface timing configuration during a session.
Default	No default

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	No default

commit

Syntax	commit
Context	config>system>sync-if-timing
Description	This command saves changes made to the system synchronous interface timing configuration.
Default	No default

Values

ql-override

Syntax	ql-override {prs stu st2 tnc st3e st3 eec1 sec prc ssu-a ssu-b eec2} no ql-override
Context	config>system>sync-if-timing>ptp config>system>sync-if-timing>ref1 config>system>sync-if-timing>ref2
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	<i>prs</i> — SONET Primary Reference Source Traceable <i>stu</i> — SONET Synchronous Traceability Unknown <i>st2</i> — SONET Stratum 2 Traceable <i>tnc</i> — SONET Transit Node Clock Traceable <i>st3e</i> — SONET Stratum 3E Traceable <i>st3</i> — SONET Stratum 3 Traceable <i>eec1</i> — Ethernet Equipment Clock Option 1 Traceable (sdh) <i>eec2</i> — Ethernet Equipment Clock Option 2 Traceable (sonet) <i>prc</i> — SDH Primary Reference Clock Traceable <i>ssu-a</i> — SDH Primary Level Synchronization Supply Unit Traceable <i>ssu-b</i> — SDH Second Level Synchronization Supply Unit Traceable <i>sec</i> — 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. This command turns -on or turns-off SSM encoding as a means of timing reference selection.
Default	no ql-selection

ref-order

Syntax	ref-order <i>first second [third]</i> no ref-order
Context	config>system>sync-if-timing
Description	The synchronous equipment timing subsystem can lock to different timing reference inputs, those specified in the ref1, ref2 command configuration. This command organizes the priority order of the timing references. If a reference source is disabled, then the clock from the next reference source as defined by ref-order is used. If all reference sources are disabled, then clocking is derived from a local oscillator. Note that 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. Only SFP based Ethernet ports can be used for reference in the current release. NOTE: If PTP is specified as reference, then the other reference cannot be specified as syncE. In other words use of PTP and syncE as a reference is mutually exclusive. The no form of the command resets the reference order to the default values. Note: Ref1 has to be configured to use one of the ports from 1/1/1 up to 1/1/4 and ref2 should be configured to use either 1/1/5 or 1/1/6. The software enforces this check. The ports 1/1/7 up to 1/1/10 can be configured as either ref1 or ref2.
Default	ref1 ref2 ptp
Parameters	

ref1

Syntax	ref1
Context	config>system>sync-if-timing
Description	This command enables the context to configure parameters for the first timing reference.

ref2

Syntax	ref2
Context	config>system>sync-if-timing
Description	This command enables the context to configure parameters for the second timing reference.

revert

Syntax	[no] revert
Context	config>system>sync-if-timing
Description	This command allows the clock to revert to a higher priority reference if the current reference goes offline or becomes unstable. If revertive switching is enabled, the highest-priority valid timing reference will be used. If a reference with a higher priority becomes valid, a reference switch over to that reference will be 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 this reference becomes invalid, a reference switch over to a valid reference with the highest priority will be initiated. When the failed reference becomes operational, it is eligible for selection.
Default	no revert

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	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. The no form of the command deletes the source port from the reference.
Parameters	<i>port-id</i> — Identify the physical port in the <i>slot/mda/port</i> format.

Generic Commands

shutdown

Syntax	[no] shutdown
Context	config>system>time>sntp config>system>sync-if-timing>ptp
Description	This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted. The no form of this command administratively enables an entity. Unlike other commands and parameters where the default state is not indicated in the configuration file, the shutdown and no shutdown states are always indicated in system generated configuration files. The no form of the command places an entity in an administratively enabled state.

description

Syntax	description <i>description-string</i> no description
Context	config>system>persistence>sub-mgmt config>system>persistence>dhcp-server
Description	The command allows the user to configure a 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.

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	none

check-golden-bootstrap

Syntax	check-golden-bootstrap
Context	admin
Description	This command validates the current golden bootstrap image, and displays its version, if found to be valid. If the golden bootstrap image is not found to be a valid, an error message is displayed to that effect.

debug-save

Syntax	debug-save <i>file-url</i>																
Context	admin																
Description	This command saves existing debug configuration. Debug configurations are not preserved in configuration saves.																
Default	none																
Parameters	<i>file-url</i> — The file URL location to save the debug configuration.																
Values	<table> <tr> <td>file url:</td><td>local-url remote-url: 255 chars max</td></tr> <tr> <td>local-url:</td><td>[<cflash-id>/ <usb-flash-id>][file-path], 200 chars max, including the cflash-id directory length, 99 chars max each</td></tr> <tr> <td>remote-url:</td><td>[{ftp://} login:pswd@remote-locn/][file-path]</td></tr> <tr> <td></td><td>remote-locn [<i>hostname</i> <i>ipv4-address</i>]</td></tr> <tr> <td></td><td>ipv4-address a.b.c.d</td></tr> <tr> <td></td><td>255 chars max, directory length 99 chars max each</td></tr> <tr> <td>cflash-id:</td><td>cf1:</td></tr> <tr> <td>usb-flash-id</td><td>uf1:</td></tr> </table>	file url:	local-url remote-url: 255 chars max	local-url:	[<cflash-id>/ <usb-flash-id>][file-path], 200 chars max, including the cflash-id directory length, 99 chars max each	remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]		remote-locn [<i>hostname</i> <i>ipv4-address</i>]		ipv4-address a.b.c.d		255 chars max, directory length 99 chars max each	cflash-id:	cf1:	usb-flash-id	uf1:
file url:	local-url remote-url: 255 chars max																
local-url:	[<cflash-id>/ <usb-flash-id>][file-path], 200 chars max, including the cflash-id directory length, 99 chars max each																
remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]																
	remote-locn [<i>hostname</i> <i>ipv4-address</i>]																
	ipv4-address a.b.c.d																
	255 chars max, directory length 99 chars max each																
cflash-id:	cf1:																
usb-flash-id	uf1:																

disconnect

Syntax	disconnect { address <i>ip-address</i> username <i>user-name</i> console telnet ftp ssh }															
Context	admin															
Description	This command disconnects a user from a console, Telnet, FTP, or SSH session. If any of the console, Telnet, FTP, or SSH options are specified, then only the respective console, Telnet, FTP, or SSH sessions are affected. If no console, Telnet, FTP, or SSH options are specified, then all sessions from the IP address or from the specified user are disconnected. Any task that the user is executing is terminated. FTP files accessed by the user will not be removed. A major severity security log event is created specifying what was terminated and by whom.															
Default	none — No disconnect options are configured.															
Parameters	address <i>ip-address</i> — The IP address to disconnect, specified in dotted decimal notation. <table><tr><td>Values</td><td>ipv4-address</td><td>a.b.c.d</td></tr><tr><td></td><td>ipv6-address</td><td>- x:x:x:x:x:x:x:x (eight 16-bit pieces)</td></tr><tr><td></td><td></td><td>x:x:x:x:x:x:d.d.d.d</td></tr><tr><td></td><td></td><td>x - [0..FFFF]H</td></tr><tr><td></td><td></td><td>d - [0..255]D</td></tr></table> username <i>user-name</i> — 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.	Values	ipv4-address	a.b.c.d		ipv6-address	- x:x:x:x:x:x:x:x (eight 16-bit pieces)			x:x:x:x:x:x:d.d.d.d			x - [0..FFFF]H			d - [0..255]D
Values	ipv4-address	a.b.c.d														
	ipv6-address	- x:x:x:x:x:x:x:x (eight 16-bit pieces)														
		x:x:x:x:x:x:d.d.d.d														
		x - [0..FFFF]H														
		d - [0..255]D														

display-config

Syntax	display-config [detail index]
Context	admin
Description	This command displays the system's running configuration. By default, only non-default settings are displayed. Specifying the detail option displays all default and non-default configuration parameters.
Parameters	detail — Displays default and non-default configuration parameters. index — Displays only persistent-indices.

reboot

Syntax	reboot [upgrade][auto-init] [now]
Context	admin
Description	This command is used only to reboot the system or initiate an upgrade of the firmware along with a reboot of the node or initiate an autoinit boot procedure along with a reboot of the node. If no options are specified, the user is prompted to confirm the reboot operation. For example: <pre>ALA-1>admin# reboot Are you sure you want to reboot (y/n)?</pre> If the now option is specified, boot confirmation messages appear.
Parameters	upgrade — Enables card firmware (CPLD and ROM) to be upgraded during chassis reboot. The 7210 SAS OS and the boot.tim support functionality to perform automatic firmware upgrades. The automatic upgrade must be enabled in the 7210 SAS OS Command Line Interface (CLI) when rebooting the system. When the upgrade keyword is specified, a chassis flag is set for the BOOT Loader (boot.tim) and on the subsequent boot of the 7210 SAS OS on the chassis, any firmware images requiring upgrading will be upgraded automatically. If an 7210 SAS is rebooted with the admin reboot command (without the upgrade keyword), the firmware images are left intact. During any firmware upgrade, automatic or manual, it is imperative that during the upgrade procedure: • Power must NOT be switched off or interrupted. • The system must NOT be reset. • No cards are inserted or removed. Any of the above conditions may render cards inoperable requiring a return of the card for resolution. now — Forces a reboot of the router immediately without an interactive confirmation. auto-init — Specifies to reset the BOF and initiates a reboot.

save

Syntax	save [<i>file-url</i>] [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.
```

By default, the running configuration is saved to the primary configuration file.

Parameters

file-url — The file URL location to save the configuration file.

Default	The primary configuration file location.		
Values	<file-url>	:	<local-url> <remote-url> - [255 chars max]
	local-url	-	[<cflash-id>/ <usb-flash-id>][file-path]
	remote-url	-	[{ftp:// tftp://} <login>:<pswd>@<remote-locn>/][<file-path>]
	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	-	cfl:
	usb-flash-id	-	ufl:

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.

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 Alcatel-Lucent Technical Assistance Center (TAC).

tech-support

Syntax	tech-support <i>file-url</i>
Context	admin
Description	This command creates a system core dump. NOTE: This command should only be used with authorized direction from the Alcatel-Lucent Technical Assistance Center (TAC).

file-url — The file URL location to save the binary file.

file url:	local-url remote-url: 255 chars max
local-url:	[<cflash-id>/ <usb-flash-id>][file-path], 200 chars max, including the cflash-id directory length, 99 chars max each
remote-url:	[{ftp://} login:pswd@remote-locn/][file-path] remote-locn [<i>hostname</i> <i>ipv4-address</i>] ipv4-address a.b.c.d 255 chars max, directory length 99 chars max each
cflash-id:	cfl:
usb-flash-id	ufl:

update-golden-bootstrap

Syntax	update-golden-bootstrap [<i>file-url</i>]									
Context	admin									
Description	This command updates the golden bootstrap image with the file-url, after validating it as a bootstrap image for the 7210 SAS platforms.Only on 7210 SAS-D newer platforms, the admin>update-golden-bootstrap CLI command does not update the golden-bootstrap image with the boot.tim specified in the parameter value, if the boot.tim is not a newer image.									
Default	cfl:/boot.tim									
Parameters	<i>file-url</i> — Specifies the file URL.									
Values	<table><tr><td>file-url:</td><td>local-url:</td><td>255 characters max</td></tr><tr><td></td><td>local-url:</td><td>[cflash-id/][file-path]</td></tr><tr><td></td><td>cflash-id:</td><td>cfl:</td></tr></table>	file-url:	local-url:	255 characters max		local-url:	[cflash-id/][file-path]		cflash-id:	cfl:
file-url:	local-url:	255 characters max								
	local-url:	[cflash-id/][file-path]								
	cflash-id:	cfl:								

System Alarm Contact Commands

Note: System Alarm Contact commands are not supported on 7210 SAS-D devices.

alarm-contact-input

Syntax	alarm-contact-input <i>alarm-contact-input-id</i>
Context	config>system>alarm-contact-input
Description	This command provides the context to configure one of four available alarm contact input pins.
Default	None
Parameters	<i>alarm-contact-input-id</i> — Identifies the alarm contact input pin. Values 1 — 4

alarm-output-severity

Syntax	[[no] alarm-output-severity { <i>critical</i> <i>major</i> <i>minor</i> <i>none</i> }
Context	config>system>alarm-contact-input
Description	This command allows the user to relay alarms from the alarm-contact input to the alarm-contact output by associating an appropriate alarm-contact output with the alarm-contact input. The system generates or clears the alarm-contact output when it triggers or clears the alarm for the associated alarm-contact input. If multiple alarm-contact input pins share an alarm-contact output, the system generates the alarm-contact output even if any one of the alarm-contact input is triggered and the system clears alarm-contact output only when all the alarm-contact input pins are cleared. The severity parameter configured by the user determines the appropriate alarm-contact output to be used for generation and clearing the alarm. Note: The system relays the alarm-contact input to the appropriate alarm-contact output only if the alarm-contact output is available on the platform.
Default	Major
Parameters	<i>critical</i> — A critical alarm output is generated or cleared. <i>major</i> — A major alarm output is generated or cleared. <i>minor</i> — A minor alarm output is generated or cleared. <i>none</i> — No alarm output is generated or cleared.

clear-alarm-msg

Syntax	[no] clear-alarm-msg {alarm-msg-text}
Context	config>system>alarm-contact-input <i>alarm-contact-input-id</i>
Description	This command allows the user to configure a text message for use along with SNMP trap and Log message that are sent when the system clears an alarm. The system generates a default message if the message is not configured. The system does not generate a trap or log if no form of the command is enabled.
Default	None
Parameters	<i>alarm-msg-text</i> — A printable character string, up to 160 characters in length.

description

Syntax	description description-string
Context	config>system>alarm-contact-input <i>alarm-contact-input-id</i> description
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.
Default	None

normal-state

Syntax	normal-state [open closed]
Context	config>system>alarm-contact-input <i>alarm-contact-input-id</i>
Description	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 is back to the normal state.
Default	closed
Parameters	<i>open</i> — 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. <i>closed-state</i> — The normal-state is identified as ‘closed’. When the system detects a transition to the ‘open’ state, and alarm is generated. The alarm is cleared when the system detects a transition back to the ‘closed’ state.

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 for the alarm-contact-input, 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	[no] trigger-alarm-msg {alarm-msg-text}
Context	config>system>alarm-contact-input <i>alarm-contact-input-id</i>
Description	This command allows the user to configure a text message for use along with SNMP trap and Log message that are sent when the system generates an alarm. The system generates a default message if the message is not configured. The system does not generate a trap or log if no form of the command is enabled.
Default	None
Parameters	<i>alarm-msg-text</i> — A printable character string, up to 160 characters in length.

LLDP System Commands

lldp

Syntax	lldp
Context	config>system
Description	This command enables the context to configure system-wide Link Layer Discovery Protocol parameters.

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.				
Parameters	<i>time</i> — Specifies the fast transmission period in seconds. <table><tr><td>Values</td><td>1 — 3600</td></tr><tr><td>Default</td><td>1</td></tr></table>	Values	1 — 3600	Default	1
Values	1 — 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.				
Parameters	<i>count</i> — Specifies the number of LLDPDUs to send during the fast transmission period. <table><tr><td>Values</td><td>1 — 8</td></tr><tr><td>Default</td><td>4</td></tr></table>	Values	1 — 8	Default	4
Values	1 — 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.
Parameters	<i>time</i> — Specifies the minimum time, in seconds, between change notifications.
Values	5 — 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.
Parameters	<i>time</i> — Specifies the time, in seconds, before re-initializing LLDP on a port.
Values	1 — 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.
Parameters	<i>count</i> — Specifies the maximum consecutive LLDPDUs transmitted.
Values	1 — 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.
Parameters	<i>multiplier</i> — Specifies the multiplier of the tx-interval. Values 2 — 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.
Parameters	<i>interval</i> — Specifies the LLDP transmit interval time. Values 1 — 100 Default 5

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.

dest-mac

Syntax	dest-mac { <i>bridge-mac</i> }
Context	config>port>ethernet>lldp
Description	This command configures destination MAC address parameters.
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 { rx tx tx-rx 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. Note that 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.

System Resource-Profile Commands

resource-profile

Syntax	resource-profile
Context	configure>system
Description	This command enables the context to configure resource-profile parameters on the system.

egress-internal-tcam

Syntax	egress-internal-tcam
Context	configure>system>resource-profile
Description	This command provides the context to allocate egress internal TCAM resources.

acl-sap-egress

Syntax	[no] acl-sap-egress				
Context	configure>system>resource-profile>egress-internal-tcam				
Description	This command allows the user to allocate maximum resources for use by egress filter policies using any of the supported match criteria. This command limits the total amount of chunks allocated for use by egress filter policies to the value specified by num-resources. In other words, the cumulative sum of chunks allocated to different match criteria supported by filter policies cannot exceed the value configured with num-resources. With the no form of the command, software does not allocate any resources for use by egress filter policies. If no resources are allocated for use, then the software fails all attempts to associate a service entity (For example: SAP, IP interface, etc) with a filter policy using any of the match criteria.				
Parameters	<i>num-resources</i> — Specifies the amount of resources that can be allocated for use by ACL policies. <table><tr><td>Values</td><td>[0-2]</td></tr><tr><td>Default</td><td>2</td></tr></table>	Values	[0-2]	Default	2
Values	[0-2]				
Default	2				

ipv6-128bit-match-enable

Syntax	[no] ipv6-128bit-match-enable <i>num-resources</i>				
Context	configure>system>resource-profile>egress-internal-tcam>acl-sap-egress				
Description	This command allows the user to allocate maximum resources for use by egress filter policies using ipv6 criteria with 128-bit IPv6 addresses. The resources cannot be shared with any other egress filter policies that specify other match criteria. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use. With the no form of the command, the software does not allocate any resources for use by egress filter policies using ipv6 criteria with 128-bit IPv6 addresses. If no resources are allocated for use, then the software fails all attempts to associate a service entity (e.g. SAP, IP interface, etc.) with a filter policy using this match criteria.				
Default	no ipv6-128bit-match-enable				
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria. <table> <tr> <td>Values</td><td>[0 2]</td></tr> <tr> <td>Default</td><td>0</td></tr> </table> NOTE: A value of 1 cannot be used.	Values	[0 2]	Default	0
Values	[0 2]				
Default	0				

mac-ipv4-match-enable

Syntax	[no] mac-ipv4-match-enable <i>num-resources</i>				
Context	configure>system>resource-profile>egress-internal-tcam>acl-sap-egress				
Description	This command allows the user to allocate maximum resources for use by egress filter policies using IPv4 criteria or MAC criteria. The resources allocated are allocated on a first-cum-first-serve basis among service entities (For example: SAP, IP interface, etc) using IPv4 and MAC criteria egress filter policies. The resources cannot be shared with any other egress filter policies that specify other match criteria. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use. With the no form of the command, the software does not allocate any resources for use by egress filter policies using MAC or IPv4 criteria. If no resources are allocated for use, then the software fails all attempts to associate a service entity (e.g. SAP, IP interface, etc.) with a filter policy using this match criteria.				
Default	mac-ipv4-match-enable 2 (to maintain backward compatibility with earlier releases)				
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria. <table> <tr> <td>Values</td><td>[0 2]</td></tr> <tr> <td>Default</td><td>0</td></tr> </table>	Values	[0 2]	Default	0
Values	[0 2]				
Default	0				

mac-ipv6-64bit-match-enable

Syntax	[no] mac-ipv6-64bit-match-enable <i>num-resources</i>
Context	configure>system>resource-profile>egress-internal-tcam>acl-sap-egress
Description	This command allows the user to allocate maximum resources for use by egress filter policies using MAC criteria or IPv6 criteria using only the upper 64-bits of the IPv6 addresses. The resources allocated are allocated on a first-cum-first-serve basis among service entities (For example: SAP, IP interface, etc.) using IPv6 64-bit and MAC criteria egress filter policies. The resources cannot be shared with any other egress filter policies that specify other match criteria. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use. With the no form of the command, the software does not allocate any resources for use by egress filter policies using MAC or IPv6 64-bit criteria. If no resources are allocated for use, then the software fails all attempts to associate a service entity (e.g. SAP, IP interface, etc.) with a filter policy using this match criteria.
Default	no mac-ipv6-64bit-match-enable
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria.
Values	[0/2]

mac-match-enable

Syntax	[no] mac-match-enable
Context	configure> system> resource-profile> egress-internal-tcam> acl-sap-egress
Description	This command allows the user to allocate maximum resources for use by egress filter policies using MAC criteria. The resources allocated are allocated on a first-cum-first-serve basis among service entities (For example: SAP, IP interface, etc.) using MAC criteria egress filter policies. This option provides for use of all available resources exclusively by MAC criteria egress filter policies and provide larger number of policies to be used. The resources cannot be shared with any other egress filter policies that specify other match criteria. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use. With the no form of the command, the software does not allocate any resources for use by egress filter policies using MAC criteria. If no resources are allocated for use, then the software fails all attempts to associate a service entity (e.g. SAP, IP interface, etc.) with a filter policy using this match criteria. Note that, its possible to use MAC policies by allocating resources that are shared with other match criteria. This option allows for better scaling.
Default	no mac-match-enable
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria.
Values	[0/2]

ingress-internal-tcam

Syntax	ingress-internal-tcam
Context	configure>system>resource-profile
Description	This command provides the context to allocate ingress internal TCAM resources.

acl-sap-ingress

Syntax	[no] acl-sap-ingress								
Context	configure>system>resource-profile>ingress-internal-tcam								
Description	This command allows the user to allocate maximum resources for use by ingress filter policies using any of the supported match criteria. This command limits the total amount of chunks allocated for use by ingress filter policies to the value specified by num-resources. In other words, the cumulative sum of chunks allocated to different match criteria supported by ingress filter policies cannot exceed the value configured with num-resources. With the no form of the command, software does not allocate any resources for use by filter policies. If no resources are allocated for use, then the software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a filter policy using any of the match criteria.								
Parameters	<i>num-resources</i> — Specifies the amount of resources that can be allocated for use by ACL policies. <table> <tr> <td>Values</td><td>[0-3] only for 7210 SAS-D</td></tr> <tr> <td>Default</td><td>2</td></tr> <tr> <td>Values</td><td>[0-5] only for 7210 SAS-E</td></tr> <tr> <td>Default</td><td>max</td></tr> </table>	Values	[0-3] only for 7210 SAS-D	Default	2	Values	[0-5] only for 7210 SAS-E	Default	max
Values	[0-3] only for 7210 SAS-D								
Default	2								
Values	[0-5] only for 7210 SAS-E								
Default	max								

ipv4-ipv6-128-match-enable

Syntax	[no] ipv4-ipv6-128-match-enable
Context	configure>system>resource-profile>ingress-internal-tcam>acl-sap-ingress
Description	This command allows the user to allocate maximum resources for use by ingress filter policies using ipv6 criteria with 128-bit IPv6 addresses. The resources can be shared with IPv4 ingress filter policies. Please see the 7210 M,X Router Configuration guide for more information on how to allow filter policies using IPv4 criteria to share resources with filter policies that use IPv6 criteria with 128-bit address and resource allocation details and fields available for use. With the no form of the command, the software does not allocate any resources for use by ingress filter policies using ipv6 criteria with 128-bit IPv6 addresses. If no resources are allocated for use, then the software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a ingress filter policy using this match criteria.

Parameters *num-resources* — Specifies the maximum amount of resources for use by this filter match criteria.

Values [0-3] only for 7210 SAS-D

Default 0

Values [0-11] only for 7210 SAS-E

Default 0

max — It is a special keyword. If user specifies max, then the software allocates one chunk when the first SAP is associated with a ingress filter policy using this match criteria. It continues to allocate resources to the service entity associated with a ingress filter policy using this criteria, as long as the total amount of resources allocated does not exceed the resources allocated to ingress filter policies (configured with the command `config> system> resource-profile> ingress-internal-tcam> acl-sap-ingress` command) and chunks are available for use.

ipv4-match-enable

Syntax `[no] ipv4-match-enable`

Context `configure>system>resource-profile>ingress-internal-tcam>acl-sap-ingress`
`configure>system>resource-profile>ingress-internal-tcam>qos-sap-ingress-resource`

Description This command allows the user to allocate maximum resources for use by ingress filter policies using ipv4 criteria. Or when used under the qos-sap-ingress-resource context, its used to allocates resources for use by SAP ingress QoS policies using IPv4 criteria (any).

The resource cannot be shared with ingress filter or SAP ingress QoS filter policies using mac criteria or ipv6 criteria. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use.

With the no form of the command, the software does not allocate any resources for use by ingress filter policies or SAP ingress QoS policies using ipv4 criteria. If no resources are allocated for use, then software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a ingress filter policy or SAP ingress QoS policy using this match criteria.

Parameters *num-resources* — Specifies the maximum amount of resources for use by this filter match criteria.

Values [0 - 3|max] for 7210 SAS-D

Values [0 - 11|max] for 7210 SAS-E

max — It is a special keyword. If user specifies max, then the software allocates one chunk when the first SAP is associated with a ingress filter policy using this match criteria. It continues to allocate resources to SAPs associated with a ingress filter policy using this criteria, as long as the total amount of resources allocated does not exceed the resources allocated to ingress filter policies (configured with the command `config> system> resource-profile> ingress-internal-tcam> acl-sap-ingress` command) and chunks are available for use.

ipv6-64-only-match-enable

Syntax	[no] ipv6-64-only-match-enable
Context	configure>system>resource-profile>ingress-internal-tcam>acl-sap-ingress
Description	This command allows the user to allocate maximum resources for use by ingress filter policies using ipv6 criteria with 64-bit IPv6 addresses. Please see the 7210 M,X Router Configuration guide for more information on resource allocation details and fields available for use. The resources cannot be shared with IPv4 filter policies or IPv6 filter policies specifying 128-bit addresses. With the no form of the command, the software does not allocate any resources for use by filter policies using ipv6 criteria with 64-bit IPv6 addresses. If no resources are allocated for use, then software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a ingress filter policy using this match criteria.
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria. Values [0 - 3] for 7210 SAS-D Values [0 - 11] for 7210 SAS-E max — It is a special keyword. If user specifies max, then the software allocates one chunk when the first SAP is associated with a ingress filter policy using this match criteria. It continues to allocate resources to SAPs associated with a ingress filter policy using this criteria, as long as the total amount of resources allocated does not exceed the resources allocated to ingress filter policies (configured with the command config> system> resource-profile> ingress-internal-tcam> acl-sap-ingress command) and chunks are available for use.

mac-match-enable

Syntax	[no] mac-match-enable
Context	configure>system>resource-profile>ingress-internal-tcam>acl-sap-ingress configure>system>resource-profile>ingress-internal-tcam> qos-sap-ingress-resource
Description	This command allows the user to allocate maximum resources for use by ingress filter policies using mac criteria. Or when used under the qos-sap-ingress-resource context, its used to allocates resources for use by SAP ingress QoS policies using MAC criteria (any). The resources cannot be shared with policies that use either IPv4 or IPv6 match criteria. For more details about the resource allocation for ingress filter policy and fields available for use with ingress filter policy please refer the 7210 SAS-D/E Router Configuration user guide. For more details about the resource allocation for SAP ingress QoS policy please refer to 7210 SAS-DE QoS user guide. With the no form of the command, the software does not allocate any resources for use by ingress filter policies or SAP ingress QoS policies using mac criteria. If no resources are allocated for use, then software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a ingress filter policy or SAP ingress QoS policy using this match criteria.
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this filter match criteria.

Values [0 - 3|max] for 7210 SAS-D

Values [0 - 11|max] for 7210 SAS-E

max — It is a special keyword. If user specifies max, then the software allocates one chunk when the first SAP is associated with a ingress filter policy using this match criteria. It continues to allocate resources to SAPs associated with a ingress filter policy using this criteria, as long as the total amount of resources allocated does not exceed the resources allocated to ingress filter policies (configured with the command `config> system> resource-profile> ingress-internal-tcam> acl-sap-ingress` command) and chunks are available for use.

NOTE: In 7210 SAS-D, mac-criteria SAP ingress QoS policies get to use an additional 128 classification entries with 64 meters. These entries are allocated to mac-criteria SAP ingress QoS resource pool by default and cannot be reassigned to any another feature or any other match criteria.

dhcp-snooping-enable

Syntax	[no] dhcp-snooping-enable
Context	configure>system>resource-profile>ingress-internal-tcam
Description	This command allows the user to allocate resources for use by DHCP snooping features from the ingress internal TCAM resource pool. Before using the dhcp-snooping feature, user must allocate resources to it using this command, else software will disallow configuration of DHCP snooping command under the service. To allocate resources to the dhcp snooping features, user will need to reduce the resources used by other features, such as ingress ACLs, or SAP ingress QoS, or others, which have been allocated resources from the ingress internal tcam resource pool and allocate it to this feature. Executing this command allocates only a single chunk of resources for use by dhcp-snooping feature. The command tools>dump> system-resources can be used to check the resource usage. The sample output below shows that a single slice with 256 entries has been allocated to the DHCP snooping feature. <pre> Total Allocated Free -----+-----+----- >> DHCP Snooping Sap Entries 251 50 250</pre> With the no form of the command, software does not allocate any resources for use by dhcp snooping feature and the feature cannot be used any more. A reboot is required after executing the no form of the command for it to take effect.
Default	no dhcp-snooping-enable No resources are allocated to the DHCP snooping feature and it cannot be used.

eth-cfm

Syntax	[no] eth-cfm
Context	configure>system>resource-profile>ingress-internal-tcam
Description	This command provides the context to allocate resources for CFM UP MEPs. With the no form of the command, the software does not allocate any resources for use by CFM UP MEPs. NOTE: CFM Down MEPs does not require explicit resource allocation by user. 7210 SAS-E does not support this command.
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by eth-cfm.
Values	[0-1]

up-mep

Syntax	[no] up-mep
Context	configure>system>resource-profile>ingress-internal-tcam>eth-cfm
Description	This command provides the context to allocate resources for CFM UP MEPs. With the no form of the command, the software does not allocate any resources for use by CFM UP MEPs. If no resources are allocated for use, then software fails all attempts to configure an UP MEP. NOTE: CFM Down MEPs does not require an explicit resource allocation by the user. Only 7210 SAS-D supports resource allocation for UP MEPs.
Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by up-mep.
Values	[0-1]

ipv6-ipv4-match-enable

Syntax	ipv6-ipv4-match-enable no ipv6-ipv4-match-enable
Context	configure>system>resource-profile>qos-sap-ingress-resource
Description	User needs to allocate resources from the SAP ingress QoS resource pool for ipv6-criteria by using the command "configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> ipv6-ipv4-match-enable" before using IPv6 criteria SAP ingress QoS policies. These resources can be shared with SAP ingress policies that use IPv4 criteria. For more details about the resource allocation for ingress filter policy and fields available for use with ingress filter policy please refer the 7210 SAS-DE Router Configuration user guide. For more details about the resource allocation for SAP ingress QoS policy please refer to 7210 SAS-DE QoS user guide.

With the no form of the command, the software does not allocate any resources for use by ingress SAP QoS policies using IPv6 criteria. If no resources are allocated for use, then software fails all attempts to associate a service entity (For example: SAP, IP interface, etc.) with a ingress filter policy using this match criteria.

Parameters	<i>num-resources</i> — Specifies the maximum amount of resources for use by this SAP ingress Qos policy match criteria.
-------------------	---

Values [0 - 6] for 7210 SAS-E

Values [0 - 3] for 7210 SAS-D

max — It is a special keyword. If user specifies *max*, then the software allocates one chunk when the first SAP is associated with a SAP ingress QoS policy using this match criteria. It continues to allocate resources to SAPs associated with SAP ingress QoS policy using this criteria, as long as the total amount of resources allocated does not exceed the resources allocated to SAP ingress QoS policies (configured with the command `config> system> resource-profile> ingress-internal-team> qos-sap-ingress-resource` command) and chunks are available for use.

qos-sap-ingress-resource

Syntax qos-sap-ingress-resource
no qos-sap-ingress-resource

Context configure>system>resource-profile

Description	This command allows the user to allocate maximum resources for use by SAP ingress QoS policies using any of the supported match criteria. This command limits the total amount of chunks allocated for use by SAP ingress QoS policies to the value specified by num-resources. In other words, the cumulative sum of chunks allocated to different match criteria supported by SAP ingress QoS policies cannot exceed the value configured with num-resources.
--------------------	---

With the no form of the command, software does not allocate any resources for use by SAP ingress QoS policies.

If no resources are allocated for use, then the software fails all attempts to associate a service entity (For example: SAP, IP interface, and other service entities.) with a SAP ingress QoS policy using any of the match criteria.

Parameters	<i>num-resources</i> — Specifies the amount of resources that can be allocated for use by SAP ingress QoS policies.
-------------------	---

Values [6 - 6] for 7210 SAS-E

Default	6
----------------	----------

Values [0 - 3] for 7210 SAS-D

Default 1

sap-aggregate-meter

Syntax	[no] sap-aggregate-meter <i>num-resource</i>
Context	configure>system>resource-profile>ingress-internal-tcam>
Description	NOTE: This command is not supported on 7210 SAS-E. This command allows the user to allocate maximum resources for use by meters/policers used to implement SAP ingress aggregate meter functionality from the global pool of ingress CAM resources. Before using the command configure> service> sap> ingress> aggregate-meter-rate user must ensure that resources are allocated to aggregate meters using this command. NOTE: For the command to take effect the node must be rebooted after making the change. This command allocates meter resources from the available global ingress CAM resource pool. By default, when resources are allocated to SAP ingress QoS policy, along with the CAM classification entries, meter resources are also allocated. Hence, if user needs to use SAP aggregate meter functionality they cannot allocate all the available resources in the global resource pool to SAP ingress QoS policies and ETH-CFM UP MEP. They need to allocate some resources for use by SAP aggregate meter (or SAP ingress ACLs or G8032-fast-flood feature). By default, when resources are allocated for ingress ACLs (and G8032 in 7210-M network mode only), only classification entries are used and meters resources are not used. SAP aggregate meter resources can use meters from this pool of meter resources. In other words, SAP aggregate meters are stolen from the unused meters in the resources allocated to ingress ACLs. If user allocates resources for ingress ACLs (or for G8032-fast-flood feature in 7210-M network mode only) and then configures resources for SAP aggregate meter using this command, then the software does the following: • It does not allocate any additional chunks/resources from the available global ingress CAM resource pool to SAP aggregate meter, if it can allocate the required number of meters from the chunks/resources allocated to ingress ACLs (or from resources allocated to G8032-fast-flood in 7210-M network mode only). For example, if user has allocated 2 chunks of 512 entries each for ingress ACLs and then configures sap-aggregate-meter to use 2 chunks to use about 512 aggregate meters, then the software will not allocate any additional entries from the available global resource pool. • If the number of ingress ACL resources allocated by user is less than the number of resources assigned by the user to sap-aggregate-meter (or if no resources are allocated to G8032), then it allocates the difference from the available global ingress CAM resource pool. For example, if user has allocated 1 chunk of 512 entries for ingress ACLs and then configures sap-aggregate-meter to use 2 chunks to use about 512 aggregate meters, then the software will allocate 1 additional chunk (2 chunks required for SAP aggregate - 1 chunk allotted to ingress ACLs) for use with SAP aggregate meter. The classification entries associated with additional chunk allotted for SAP aggregate-meter can be used by the ingress ACLs policies. It cannot be used by SAP ingress QoS policies and eth-cfm UP MEP. Similar checks as above are performed when user allocates resources for SAP aggregate meters using this command and then configures resources for ingress ACLs (or for G8032-fast-flood feature). That is, the software does the following: • It does not allocate any additional entries from the available global ingress CAM resource pool to ingress ACLs, if it can allocate the required number of classification entries from the chunks

allocated to SAP aggregate meter feature. For example, if user has allocated 2 chunks of 512 entries each for SAP aggregate meters and then configures ingress ACLs to use 2 chunks to use about 512 classification entries, then the software will not allocate any additional entries from the available global resource pool.

- If the number of SAP aggregate meter resources allocated by user is less than the number of resources requested by the user for ingress ACLs, then it allocates the difference from the available global ingress CAM resource pool. For example, if user has allocated 1 chunk of 512 entries for SAP aggregate meters and then configures ingress ACLs to use 2 chunks, then the software will allocate 1 additional chunk (2 chunks required for ingress ACLs - 1 chunk allotted to SAP aggregate meter) for use with ingress ACLs. The meter resources associated with additional chunk allotted for ingress ACLs can be assigned to the SAP aggregate feature, if need be.

Please see the 7210 DE QoS user guide, 7210 DE Systems Basic Guide and the 7210 SAS-DE Router Configuration Guide for more information about use of SAP aggregate feature, ingress CAM resource allocation and use of ACLs policies respectively.

With the no form of the command, the software does not allocate any resources for use by SAP ingress aggregate meter. If no resources are allocated for use, then the software fails all attempts to associate an aggregate-meter with SAP ingress.

Parameters *num-resources* — Specifies the maximum amount of resources for use by this filter match criteria.
Values [0-1] for 7210 SAS-D

max-ipv6-routes

Syntax **[no] max-ipv6-routes** *number*
Context `configure>system>resource-profile>`
Description **NOTE:** This command is supported only on 7210 SAS-D.

This command allows the user to allocate IPv6 route entries in the L3 forwarding table.

L3 forwarding table entries is shared among IPv4 and IPv6 route entries. Before adding routes for IPv6 destinations, route entries in the routed lookup table needs to be allocated for IPv6 addresses using this command. This command allocates route entries for /64 IPv6 prefix route lookups. The remainder of the L3 forwarding table is used for IPv4 routing entries. The system does not allocate any IPv6 route entries by default and user needs to allocate some resources before using IPv6.

NOTE: For the command to take effect the node must be rebooted after making the change. Please see the example below and the Systems Basic guide for more information.

NOTE: A separate route table is used for IPv6 /128-bit prefix route lookup. A limited amount of IPv6 /128 prefixes route lookup entries is supported. The software enables lookups in this table by default (in other words no user configuration is required to enable IPv6 /128-bit route lookup).

NOTE: IPv6 IP interfaces are allowed to be created without allocating IPv6 route entries. With this only IPv6 hosts on the same IPv6 subnet will be reachable.

With the no form of the command, the software does not allocate any resources for use by IPv6 routes.

Default no max-ipv6-routes

Parameters *number* — Specifies the maximum amount of entries to be used for IPv6 routes.

Values
[1 - 6000] on 7210 SAS-D

Fan Controller Commands

fan

Syntax	fan { <i>on</i> <i>off</i> <i>auto</i> }
Context	configure>system
Description	7210 SAS-D chassis with 128MB flash has a fan to help in circulating the air inside the chassis. It does not provide for cooling. This command allows the operator to control the operation of the fan. Operators can choose to either switch 'on' or 'off' the fan permanently or let the system control the operation of the fan by setting the value to 'auto'. In auto mode, software controls the operation of the fan. It switches the fan 'on', if the system defined temperature threshold is exceeded and switches it 'off' when temperature falls back to normal. It also ensures that fan is not switched on and off more than once in 30 minutes.
Default	auto
Parameters	<i>on</i> — The operation of the fan is controlled by the user and it is always switched on/operating. <i>off</i> — The operation of the fan is controlled by the user and it is always switched off/not operating. <i>auto</i> — Values The fan is controlled by the system. It is switched on when the temperature threshold exceeds certain value and is switched off when the temperature threshold falls back below a certain value.

Show Commands

SYSTEM COMMANDS

connections

Syntax	connections [address <i>ip-address</i> [interface <i>interface-name</i>]] [port <i>port-number</i>] [detail]
Context	show>system
Description	This command displays UDP and TCP connection information. If no command line options are specified, a summary of the TCP and UDP connections displays.
Parameters	<i>ip-address</i> — Displays only the connection information for the specified IP address. Values ipv4-address: a.b.c.d (host bits must be 0) ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x.d.d.d.d x - [0..FFFF]H d - [0..255]D <i>port-number</i> — Displays only the connection information for the specified port number. Values 0 — 65535 detail — Appends TCP statistics to the display output.
Output	Standard Connection Output — The following table describes the system connections output fields.

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.

Sample Output

```

A:ALA-12# show system connections
=====
Connections :
=====

```

Proto	RecvQ	TxmtQ	Local Address	Remote Address	State
TCP	0	0	0.0.0.0.21	0.0.0.0.0	LISTEN
TCP	0	0	0.0.0.0.23	0.0.0.0.0	LISTEN
TCP	0	0	0.0.0.0.179	0.0.0.0.0	LISTEN
TCP	0	0	10.0.0.xxx.51138	10.0.0.104.179	SYN_SENT
TCP	0	0	10.0.0.xxx.51139	10.0.0.91.179	SYN_SENT
TCP	0	0	10.10.10.xxx.646	0.0.0.0.0	LISTEN
TCP	0	0	10.10.10.xxx.646	10.10.10.104.49406	ESTABLISHED
TCP	0	0	11.1.0.1.51140	11.1.0.2.179	SYN_SENT
TCP	0	993	192.168.x.xxx.23	192.168.x.xx.xxxx	ESTABLISHED
UDP	0	0	0.0.0.0.123	0.0.0.0.0	---
UDP	0	0	0.0.0.0.646	0.0.0.0.0	---
UDP	0	0	0.0.0.0.17185	0.0.0.0.0	---
UDP	0	0	10.10.10.xxx.646	0.0.0.0.0	---
UDP	0	0	127.0.0.1.50130	127.0.0.1.17185	---

```

-----
No. of Connections: 14
=====
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
=====

```

A:ALA-12#

cpu

- Syntax** **cpu** [**sample-period** *seconds*]
- Context** show>system
- Description** This command displays CPU utilization per task over a sample period.
- Parameters** **sample-period** *seconds* — The number of seconds over which to sample CPU task utilization.
- Default** 1
- Values** 1 — 5
- Output** **System CPU Output** — The following table describes the system CPU output fields.

Table 25: Show System CPU Output Fields

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	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. 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.

Sample Output

```
*A:cses-E11# show system cpu sample-period 2
=====
CPU Utilization (Sample period: 2 seconds)
=====
```

Name	CPU Time (uSec)	CPU Usage	Capacity Usage
-----	-----	-----	-----
BFD	10	~0.00%	~0.00%
Cards & Ports	8,332	0.41%	0.08%
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%
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%
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%
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#
```

cron

Syntax **cron**

Context show>cron

Description This command enters the show CRON context.

action

Syntax **action** [*action-name*] [*owner action-owner*] **run-history** *run-state*

Context show>cron#

Description This command displays cron action parameters.

Parameters **action** *action-name* — 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.

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.

```
A:sim1>show>cron schedule test
```

Label	Description
Schedule name	Displays the schedule name.
Schedule owner	Displays the owner name of the action.
Description	Displays the schedule's description.

Label	Description (Continued)
Administrative status	Enabled — The administrative status is enabled. Disabled — Administratively disabled.
Operational status	Enabled — The operational status is enabled. Disabled — Operationally disabled.
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.

Label	Description (Continued)
Last failure time	Displays the system time of the last failure.
=====	
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	

script

Syntax	script [<i>script-name</i>] [<i>owner script-owner</i>]
Context	show>cron#
Description	This command displays cron script parameters.
Parameters	<i>schedule-name</i> — Displays information for the specified script. <i>owner schedule-owner</i> — Displays information for the specified script owner.
Output	The following table describes the show cron script output fields.

Label	Description
Script	Displays the name of the script.

Label	Description (Continued)
Script owner	Displays the owner name of script.
Administrative status	Enabled — Administrative status is enabled. Disabled — Administratively abled.
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>cron# script
=====
CRON Script Information
=====
Script                : test
Owner name            : TiMOS CLI
Description           : asd
Administrative status  : enabled
Operational status    : enabled
Script source location : ftp://*****:*****@192.168.15.1/home/testlab_bgp
                      /cron/test1.cfg
Last script error     : none
Last change           : 2006/11/07 17:10:03
=====
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 **System Information Output** — The following table describes the system information output fields.

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.
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.

Label	Description (Continued)
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.
Last Booted Config File	The URL and filename of the last loaded configuration file.
Last Boot Cfg Version	The date and time of the last boot.
Last Boot Config Header	Displays header information such as image version, date built, date generated.
Last Boot Index Version	The version of the persistence index file read when the card was last rebooted.
Last Boot Index Header	The header of the persistence index file read when the 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.

Label	Description (Continued)
DNS Server	The IP address of the DNS server.
DNS Domain	The DNS domain name of the node.
BOF Static Routes	To — The static route destination. Next Hop — The next hop IP address used to reach the destination. Metric — Displays the priority of this static route versus other static routes. None — No static routes are configured.

memory-pools

Syntax	memory-pools
Context	show>system
Description	This command displays system memory status.
Output	Memory Pools Output — The following table describes memory pool output fields.

Table 26: Show Memory Pool Output Fields

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
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
IGMP	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 [{ peers peer <i>peer-address</i> } { servers server <i>server-address</i> }] [[all]] [[detail]]
Context	show>system
Description	This command displays NTP protocol configuration and state.
Output	Show NTP Output — The following table describes NTP output fields.

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

Label	Description (Continued)
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.
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.
Outlyer	The peer is discarded as an outlyer. This peer will not be used for synchronization.
Candidate	The peer is accepted as a possible source of synchronization.
Selected	The peer is an acceptable source of synchronization, but its synchronization distance is greater than six other peers.
Chosen	The peer is chosen as the source of synchronization.
ChosenPPS	The peer is chosen as the source of synchronization, but the actual synchronization is occurring from a pulse-per-second (PPS) signal.
Remote	The IP address of the remote NTP server or peer with which this local host is exchanging NTP packets.
Reference ID	When 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:

Label	Description (Continued)
	Peer Codes: ACST — The association belongs to any cast server. AUTH — Server authentication failed. Please wait while the association is restarted. AUTO — Autokey sequence failed. Please wait while the association is restarted. BCST — The association belongs to a broadcast server. CRPT — Cryptographic authentication or identification failed. The details should be in the system log file or the cryptostats statistics file, if configured. No further messages will be sent to the server. DENY — Access denied by remote server. No further messages will be sent to the server. DROP — Lost peer in symmetric mode. Please wait while the association is restarted. RSTR — Access denied due to local policy. No further messages will be sent to the server. INIT — The association has not yet synchronized for the first time. MCST — The association belongs to a manycast server. NKEY — No key found. Either the key was never installed or is not trusted. RATE — Rate exceeded. The server has temporarily denied access because the client exceeded the rate threshold. RMOT — The association from a remote host running ntpdc has had unauthorized attempted access. STEP — A step change in system time has occurred, but the association has not yet resynchronized. System Codes INIT — The system clock has not yet synchronized for the first time. STEP — A step change in system time has occurred, but the system clock has not yet resynchronized.
St	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:pc-40>config>system>time>ntp# show system ntp
```

```
=====
```

NTP Status

```
=====
```

```

Enabled           : Yes           Stratum           : 3
Admin Status      : up            Oper Status       : up
Server enabled    : No            Server keyId      : none
System Ref Id     : 192.168.15.221 Auth Check        : Yes
=====
```

```
A:pc-40>config>system>time>ntp# show system ntp all
```

```
=====
```

NTP Status

```
=====
```

```

Enabled           : Yes           Stratum           : 3
Admin Status      : up            Oper Status       : up
Server enabled    : No            Server keyId      : none
System Ref Id     : 192.168.15.221 Auth Check        : Yes
=====
```

```
=====
```

NTP Active Associations

```
=====
```

State	Remote	Reference ID	St	Type	Auth	Poll	R	Offset
reject	192.168.15.221	192.168.14.50	2	srvr	none	64	y	0.901
chosen	192.168.15.221	192.168.14.50	2	mclnt	none	64	y	1.101

```
=====
```

```
A:pc-40>config>system>time>ntp#
```

```
*A:pc-4.0# show system ntp detail
```

```
=====
```

NTP Status

```
=====
```

```

Enabled           : Yes           Stratum           : 3
Admin Status      : up            Oper Status       : up
Server enabled    : No            Server keyId      : none
System Ref Id     : 10.135.16.130 Auth Check        : Yes
Auth Errors       : 1             Auth Errors Ignored : 0
Auth Key Id Errors : 1            Auth Key Type Errors : 0
=====
```

```
=====
```

NTP Configured Broadcast Interfaces

```
=====
```

vRouter	Interface	Address	Type	Auth	Poll
Base	new	Host-ones	bcast	no	off
Base	direct	Host-ones	bclnt	no	n/a

```
=====
```

```
*A:pc-4.0#
```

```
*A:pc-4.0# show system ntp detail all
```

```
=====
```

NTP Status

```
=====
```

```

Enabled           : Yes           Stratum           : 3
Admin Status      : up            Oper Status       : up
=====
```

```

Server enabled      : No                Server keyId       : none
System Ref Id      : 10.135.16.130     Auth Check         : Yes
Auth Errors        : 0                 Auth Errors Ignored : 0
Auth Key Id Errors : 0                 Auth Key Type Errors : 0
=====
NTP Configured Broadcast Interfaces
=====
vRouter      Interface      Address          Type    Auth    Poll
-----
Base         new            Host-ones       bcast   no      off
Base         direct          Host-ones       bclnt   no      n/a
=====
NTP Active Associations
=====
State      Remote          Reference ID     St Type  A  Poll Reach    Offset(ms)
-----
candidate  21.0.0.1             10.135.16.130   3 actpr y  64  YYYY.YY.  14.440
chosen     10.135.16.130        127.127.1.0     2 srvr  -  256  .Y.YYYYY  24.364
reject     10.135.16.130        127.127.1.0     2 bclnt -  64  .....Y  27.576
=====
*A:pc-4.0#

```

resource-profile

Syntax	resource-profile
Context	show>system
Description	This command displays the resource-profile protocol configuration and state.
Parameters	<i>active configure</i> — keyword - Displays active or configured values.
Output	Show resource-profile Output — The following table describes resource-profile output fields.

Table 27: Show system resource-profile output fields.

Label	Description
Ingress Internal CAM	Displays the applications sharing ingress CAM resource.
Sap Ingress ACL resource	Displays the resources configured for use by SAP Ingress ACL policies.
IPv4 Resource	Displays the resources configured for use by ingress ACL policies that use ipv4-criteria. Disable – No resources are allocated for use by this feature. Therefore, no policies of this type can be associated to a SAP.

Table 27: Show system resource-profile output fields.

Label	Description
IPv4-IPv6 Resource	Displays the resources configured for use by ingress ACL policies that use ipv6 128-bit address match-criteria. Disable – No resources are allocated for use by this feature. Hence, no policies of this type can be associated to a SAP.
Mac Resource	Displays the resources configured for use by ingress ACL policies that use mac-criteria. Disable – No resources are allocated for use by this feature. Hence, no policies of this type can be associated to a SAP.
IPv6-64 bit Resource	Displays the resources configured for use by ingress ACL policies that use ipv6 64-bit address match-criteria. Disable – No resources are allocated for use by this feature. Hence, no policies of this type can be associated to a SAP.
Eth CFM	Groups the context for resources consumed by Ethernet CFM applications.
up-mep	Displays the resources configured for use by UP MEP. Disable – No resources are allocated for use by this feature. Hence, no UP MEPs can be created.
Sap Ingress QoS resource	The total amount of ingress internal CAM chunks configured for use by SAP ingress classification.
Mac and IPv4 Resource	The total amount of egress internal CAM chunks configured for use by MAC and IPv4 egress ACL match criteria policies.
Mac-only Resource	The total amount of egress internal CAM chunks configured for use only by MAC egress ACL match criteria policies.
IPv6 128 bit Resource	The total amount of egress internal CAM chunks configured for use only by IPv6 egress ACL match criteria policies (128-bit IPv6 address can be specified in the match criteria).
Mac and IPv6 64 bit Resource	The total amount of egress internal CAM chunks configured for use by MAC and IPv6 egress ACL match criteria policies (only 64-bit higher order bits of the IPv6 address can be specified in the match criteria).
Sap Egress ACL resource	Displays the egress ACL resource allocation configured for various match criteria.
Egress Internal CAM	Displays the resource allocation configured for the egress internal CAM.
IPv6 FIB	Displays the amount of IPv6 FIB size configured for use by IPv6 routing.

Sample Output for 7210 SAS-D

```
*A:7210SAS>show>system# resource-profile

=====
Active System Resource Profile Information
=====
-----
IPv6 FIB
-----
max-ipv6-routes           : disable

-----
-----
Ingress Internal CAM
-----
Sap Ingress Qos resource   : 2           Sap Aggregate Meter       : 1
-----
IPv4 Resource              : max           Mac Resource              : max
IPv4-IPv6 Resource         : disable

-----
Sap Ingress ACL resource   : 1
-----
IPv4 Resource              : max           Mac Resource              : max
IPv4-IPv6 128 bit Resource : disable    IPv6 64 bit Resource       : disable

-----
Eth CFM                    : disable
-----
up-mep                    : disable

-----
-----
Egress Internal CAM
-----
Sap Egress ACL resource    : 2
-----
Mac and IPv4 Resource      : 2           Mac-only Resource         : disable
IPv6 128 bit Resource      : disable    Mac and IPv6 64 bit Resour*: disable

-----
* indicates that the corresponding row element may have been truncated.
*A:7210SAS>show>system#
```

Sample Output for 7210 SAS-E

```
A:7210SAS>show>system# resource-profile

=====
Active System Resource Profile Information
=====
-----
Ingress Queue Mode         : none
-----
-----
Ingress Internal CAM
```

```

-----
Sap Ingress Qos resource   : 6
-----
IPv4 Resource              : max          Mac Resource              : max
IPv4-IPv6 Resource        : disable
-----
Sap Ingress ACL resource   : 5
-----
IPv4 Resource              : max          Mac Resource              : max
IPv4-IPv6 128 bit Resource : disable    IPv6 64 bit Resource        : disable
-----
-----
Egress Internal CAM
-----
Sap Egress ACL resource    : 2
-----
Mac and IPv4 Resource      : 1          Mac-only Resource          : 1
IPv6 128 bit Resource      : disable    Mac and IPv6 64 bit Resour*: disable
-----
=====
* indicates that the corresponding row element may have been truncated.
*A:SASE>show>system#A:7210SAS>show>system#

```

ptp

Syntax `ptp [ peer <ip-address> [detail] | peers [detail] | unicast | statistics | standby ]`

Context `show>system`

Description

Sample Output:

```

A:7210SAS>show>system# ptp

=====
IEEE 1588/PTP Clock Information
=====
-----
Local Clock
-----
Clock Type      : boundary          PTP Profile      : IEEE 1588-2008
Domain         : 0                  Network Type     : sdh
Admin State    : up                 Oper State       : up
Clock Id       : 4c5fd2fffe29049e   Clock Class      : 248 (default)
Clock Accuracy  : unknown           Clock Variance   : ffff (not computed)
Clock Priority1 : 128                Clock Priority2   : 128
PTP Recovery State: disabled
Frequency Offset : n/a

```

```
-----
Parent Clock
-----
IP Address       : 221.0.0.2
Parent Clock Id  : 4c5fd2fffe295072   Remote PTP Port   : 5
GM Clock Id      : 00b0aeffffe02e5e5   GM Clock Class    : 6
GM Clock Accuracy : within 100 ns       GM Clock Variance  : 0x6400 (3.7E-09)
GM Clock Priority1: 128                 GM Clock Priority2 : 128
=====
Time Information
-----
Timescale        : PTP
Current Time     : 2012/12/13 11:05:43 (UTC)
Frequency Traceable : yes
Time Traceable   : yes
Time Source      : GPS
=====
A:7210SAS>show>system#
```

sntp

- Syntax** **sntp**
- Context** show>system
- Description** This command displays SNTP protocol configuration and state.
- Output** **Show SNTP Output** — The following table describes SNTP output fields.

Table 28: Show System SNTP Output Fields

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:pc-4.0# show system sntp
```

```

=====
SNTP Status
=====
Admin Status : up           Oper Status : up           Mode : broadcast
=====
SNTP Servers
=====
SNTP Server      Version      Preference      Interval
-----
10.135.16.90     3            Preferred       64
-----
No. of SNTP Servers: 1
=====
*A:pc-4.0#

```

thresholds

Syntax	thresholds
Context	show>system
Description	This command display system monitoring thresholds.
Output	Thresholds Output — following table describes system threshold output fields.

Label	Description
Variable	Displays the variable OID.
Alarm Id	Displays the numerical identifier for the alarm.
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.
Sample Type	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.

Label	Description (Continued)
Last Sent	Displays the date and time the alarm was sent.
Action Type	log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command. 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 a entry in the RMON-MIB logTable and a TiMOS logger event are generated. none — No action is taken
Owner	Displays the owner of the event.

Sample Output

```
A:ALA-48# show system thresholds
=====
Threshold Alarms
=====
Variable: tmnxCpmFlashUsed.1.11.1
Alarm Id      : 1      Last Value : 835
Rising Event Id : 1      Threshold  : 5000
Falling Event Id : 2      Threshold  : 2500
Sample Interval : 2147483* SampleType : absolute
Startup Alarm   : either Owner       : TiMOS CLI
Variable: tmnxCpmFlashUsed.1.11.1
Alarm Id      : 2      Last Value : 835
Rising Event Id : 3      Threshold  : 10000
Falling Event Id : 4      Threshold  : 5000
Sample Interval : 2147483* SampleType : absolute
Startup Alarm   : rising Owner       : TiMOS CLI
Variable: sgiMemoryUsed.0
Alarm Id      : 3      Last Value : 42841056
Rising Event Id : 5      Threshold  : 4000
Falling Event Id : 6      Threshold  : 2000
Sample Interval : 2147836 SampleType : absolute
Startup Alarm   : either Owner       : TiMOS CLI
=====
* indicates that the corresponding row element may have been truncated.
=====
Threshold Events
=====
Description: TiMOS CLI - cflash capacity alarm rising event
Event Id      : 1      Last Sent   : 10/31/2006 08:47:59
Action Type    : both   Owner       : TiMOS CLI
Description: TiMOS CLI - cflash capacity alarm falling event
Event Id      : 2      Last Sent   : 10/31/2006 08:48:00
Action Type    : both   Owner       : TiMOS CLI
Description: TiMOS CLI - cflash capacity warning rising event
Event Id      : 3      Last Sent   : 10/31/2006 08:47:59
```



```

Action Type      : both      Owner       : TiMOS CLI
Description: TiMOS CLI - cflash capacity warning falling event
Event Id        : 4          Last Sent   : 10/31/2006 08:47:59
Action Type      : both      Owner       : TiMOS CLI
Description: TiMOS CLI - memory usage alarm rising event
Event Id        : 5          Last Sent   : 10/31/2006 08:48:00
Action Type      : both      Owner       : TiMOS CLI
Description: TiMOS CLI - memory usage alarm falling event
Event Id        : 6          Last Sent   : 10/31/2006 08:47:59
Action Type      : both      Owner       : TiMOS CLI
=====
Threshold Events Log
=====
Description      : TiMOS CLI - cflash capacity alarm falling eve
                  nt : value=835, <=2500 : alarm-index 1, event
                  -index 2 alarm-variable OID tmnxCpmFlashUsed.
                  1.11.1
Event Id         : 2          Time Sent   : 10/31/2006 08:48:00
Description      : TiMOS CLI - memory usage alarm rising event :
                  value=42841056, >=4000 : alarm-index 3, even
                  t-index 5 alarm-variable OID sgiMemoryUsed.0
Event Id         : 5          Time Sent   : 10/31/2006 08:48:00
=====
A:ALA-48#

```

time

Syntax	time
Context	show>system
Description	This command displays the system time and zone configuration parameters.
Output	System Time Output — The following table describes system time output fields.

Table 29: Show System Time Output Fields

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.
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—60) added to the time at the beginning of Daylight Saving Time and subtracted at the end Daylight Saving Time.
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#

vwm-shelf

Syntax **vwm-shelf** *vwm-shelf-id* [all] [detail]

Context show>system

Description List all the shelves connected to the 7210 SAS node and display the administrative and operational state of the connected shelves.

VWM-Shelf output — The following table describes the VWM-shelf output fields.

Table 30: Show VWM-shelf Output Fields

Label	Description
Shelf-ID	Configured shelf-ID for the 1830 VWM shelf connected to the 7210. It must match the rotary dial setting on the 1830 device.
USB/l2C	Type of connection used to connect to the 1830 VWM shelf.
Admin State	The administrative state of the shelf. It is shown as UP if user has enabled the shelf in the configuration.
Oper State	Operational state of the shelf. It is set to up if the admin state is UP and the 7210 node is able to communicate successfully with the shelf.
Number of Equipped slots	Number of line cards in use on the shelf.

Sample Output

```
*A:7210SAS>show>system# vwm-shelf

=====
Shelf Summary
=====
Shelf-ID      USB/      Admin      Oper      Number of
              I2C       State      State     Equipped slots
-----
7             USB       UP         UP        2
=====

*A:7210SAS>show>system#
```

time

Syntax	time
Context	show
Description	This command displays the current day, date, time and time zone. The time is displayed either in the local time zone or in UTC depending on the setting of the root level time-display command for the console session.
Output	Sample Output <pre>A:ALA-49# show time Tue Oct 31 12:17:15 GMT 2006</pre>

tod-suite

Syntax	tod-suite [detail] tod-suite associations tod-suite failed-associations
Context	show>cron
Description	This command displays information on the configured time-of-day suite.
Output	CRON TOD Suite Output — The following table describes TOD suite output fields:

Table 31: Show System tod-suite Output Fields

Label	Description
Associations	Shows which SAPs this tod-suite is associated with.
failed-associations	Shows the SAPs or Multiservice sites where the TOD Suite could not be applied successfully.
Detail	Shows the details of this tod-suite.

Sample Output

```

A:kerckhot_4# show cron tod-suite suite_sixteen detail
=====
Cron tod-suite details
=====
Name           : suite_sixteen
Type / Id      Time-range      Prio  State
-----
Ingress Qos Policy
  1160          day             5     Inact
  1190          night          6     Activ
Ingress Scheduler Policy
  SchedPolCust1_Day      day             5     Inact
  SchedPolCust1_Night    night          6     Activ
Egress Qos Policy
  1160          day             5     Inact
  1190          night          6     Activ
Egress Scheduler Policy
  SchedPolCust1Egress_Day day             5     Inact
=====
A:kerckhot_4#

The following example shows output for TOD suite associations.

A:kerckhot_4# show cron tod-suite suite_sixteen associations
=====
Cron tod-suite associations for suite suite_sixteen
=====
Service associations

```

```

-----
Service Id   : 1                               Type    : VPLS
SAP 1/1/1:1
SAP 1/1/1:2
SAP 1/1/1:3
SAP 1/1/1:4
SAP 1/1/1:5
SAP 1/1/1:6
SAP 1/1/1:20
-----

```

```

Number of SAP's : 7
Customer Multi-Service Site associations
-----

```

```

Multi Service Site: mss_1_1
-----

```

```

Number of MSS's: 1
=====

```

```

A:kerckhot_4#

```

The following example shows output for TOD suite failed-associations.

```

A:kerckhot_4# show cron tod-suite suite_sixteen failed-associations
=====

```

```

Cron tod-suite associations failed
=====

```

```

tod-suite suite_sixteen : failed association for SAP
-----

```

```

Service Id   : 1                               Type    : VPLS
SAP 1/1/1:2
SAP 1/1/1:3
SAP 1/1/1:4
SAP 1/1/1:5
SAP 1/1/1:6
SAP 1/1/1:20
-----

```

```

tod-suite suite_sixteen : failed association for Customer MSS
-----

```

```

None
-----

```

```

Number of tod-suites failed/total : 1/1
=====

```

```

A:kerckhot_4#

```

Zooming in on one of the failed SAPs, the assignments of QoS and scheduler policies are shown as not as intended:

```

A:kerckhot_4# show service id 1 sap 1/1/1:2
=====

```

```

Service Access Points(SAP)
=====

```

```

Service Id      : 1
SAP             : 1/1/1:2                      Encap         : q-tag
Dot1Q Ethertype : 0x8100                      QinQ Ethertype : 0x8100
Admin State     : Up                          Oper State    : Up
Flags           : None
Last Status Change : 10/05/2006 18:11:34
Last Mgmt Change  : 10/05/2006 22:27:48
Max Nbr of MAC Addr: No Limit                  Total MAC Addr : 0

```

Learned MAC Addr	: 0	Static MAC Addr	: 0
Admin MTU	: 1518	Oper MTU	: 1518
Ingress qos-policy	: 1130	Egress qos-policy	: 1130
Intend Ing qos-pol*	: 1190	Intend Egr qos-po*	: 1190
Shared Q plcy	: n/a	Multipoint shared	: Disabled
Ingr IP Fltr-Id	: n/a	Egr IP Fltr-Id	: n/a
Ingr Mac Fltr-Id	: n/a	Egr Mac Fltr-Id	: n/a
tod-suite	: suite_sixteen	qinq-pbit-marking	: both
Egr Agg Rate Limit	: max		
ARP Reply Agent	: Unknown	Host Conn Verify	: Disabled
Mac Learning	: Enabled	Discard Unkwn Srce	: Disabled
Mac Aging	: Enabled	Mac Pinning	: Disabled
L2PT Termination	: Disabled	BPDU Translation	: Disabled

Multi Svc Site	: None		
I. Sched Pol	: SchedPolCust1		
Intend I Sched Pol	: SchedPolCust1_Night		
E. Sched Pol	: SchedPolCust1Egress		
Intend E Sched Pol	: SchedPolCust1Egress_Night		
Acct. Pol	: None	Collect Stats	: Disabled
Anti Spoofing	: None	Nbr Static Hosts	: 0

=====

A:kerckhot_4#

If a time-range is specified for a filter entry, use the **show filter** command to view results:

A:kerckhot_4# show filter ip 10

=====

IP Filter

Filter Id	: 10	Applied	: No
Scope	: Template	Def. Action	: Drop
Entries	: 2		

Filter Match Criteria : IP

Entry	: 1010	Cur. Status	: Inactive
time-range	: day		
Log Id	: n/a		
Src. IP	: 0.0.0.0/0	Src. Port	: None
Dest. IP	: 10.10.100.1/24	Dest. Port	: None
Protocol	: Undefined	Dscp	: Undefined
ICMP Type	: Undefined	ICMP Code	: Undefined
Fragment	: Off	Option-present	: Off
Sampling	: Off	Int. Sampling	: On
IP-Option	: 0/0	Multiple Option	: Off
TCP-syn	: Off	TCP-ack	: Off
Match action	: Forward		
Next Hop	: 138.203.228.28		
Ing. Matches	: 0	Egr. Matches	: 0
Entry	: 1020		
time-range	: night	Cur. Status	: Active
Log Id	: n/a		
Src. IP	: 0.0.0.0/0	Src. Port	: None
Dest. IP	: 10.10.1.1/16	Dest. Port	: None
Protocol	: Undefined	Dscp	: Undefined
ICMP Type	: Undefined	ICMP Code	: Undefined
Fragment	: Off	Option-present	: Off
Sampling	: Off	Int. Sampling	: On

```
IP-Option      : 0/0                      Multiple Option: Off
TCP-syn        : Off                      TCP-ack       : Off
Match action   : Forward
Next Hop       : 172.22.184.101
Ing. Matches   : 0                      Egr. Matches   : 0
=====
A:kerckhot_4#

If a filter is referred to in a TOD Suite assignment, use the show filter associations command to view the output:

A:kerckhot_4# show filter ip 160 associations
=====
IP Filter
=====
Filter Id      : 160                      Applied       : No
Scope         : Template                 Def. Action   : Drop
Entries       : 0
-----
Filter Association : IP
-----
Tod-suite "english_suite"
- ingress, time-range "day" (priority 5)
=====
A:kerckhot_4#
```

time-range

- Syntax** `time-range name associations [detail]`
- Context** `show>cron`
- Description** This command displays information on the configured time ranges.
- Output** **Time Range Output —** The following table displays system time range output fields:

Table 32: Show System Time-range Output Fields

Label	Description
Associations	Shows the time-range as it is associated with the TOD suites and ACL entries as well as the SAPs using them.
Detail	Shows the details of this time-range.

Sample Output

The following example shows time-range detail output.

```
A:ala# show cron time-range time-range2 detail
=====
Cron time-range
=====
Name      : time-range1
Periodic  : Start * * * * End * * * *
```



```
Absolute      : Start * * * * End * * * *
```

The following example shows output for time-range associations with previously created IP and MAC filters.

```
A:ala# show cron time-range day associations
=====
Cron time-range associations
=====
Name           : day                               State  : Inactive
-----
IP Filter associations
-----
IP filter Id   : 10, entry 1010
-----
MAC Filter associations
-----
None
-----
Tod-suite associations
-----
Tod-suite : suite_sixteen, for Ingress Qos Policy "1160"
Tod-suite : suite_sixteen, for Ingress Scheduler Policy "SchedPolCust1_Day"
Tod-suite : suite_sixteen, for Egress Qos Policy "1160"
Tod-suite : suite_sixteen, for Egress Scheduler Policy "SchedPolCust1Egress_Day"
=====
```

uptime

Syntax	uptime
Context	show
Description	This command displays the time since the system started.
Output	Uptime Output — The following table describes uptime output fields.

Table 33: System Timing Output Fields

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#
```

sync-if-timing

Syntax	sync-if-timing
Context	show>system
Description	This command displays synchronous interface timing information.
Output	System Timing Output — The following table describes sync-if-timing output fields.

Label	Description
System Status CPM A	Indicates the system status of CPM A.
Reference Input Mode	Indicates the reference input mode.
Reference Order	Indicates the reference order.
Reference Input 1	Displays information about reference input 1
Admin Status	down — Indicates the ref1 or ref2 configuration is administratively shutdown. up — Indicates the ref1 or ref2 configuration is administratively enabled. diag — Indicates the reference has been forced using the force-reference command.
Qualified for Use	Indicates if the reference input 1 (or input 2) is qualified for use.
Selected for Use	Indicates if reference input 1(or input 2) is selected for use.
Source Port	Displays the source port information.
Reference Input 2	Displays information about reference input 2.
Not Selected Due to	Indicates the reason if reference input 2 is not selected. Note: SSM supported only on 7210 SAS-D devices.
Quality Level Selection	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.
System Quality Level	Indicates the quality level being generated by the system clock.
Rx Quality Level	Indicates the QL value received on the interface. • inv - SSM received on the interface indicates an invalid code for the interface type. • unknown - No QL value was received on the interface.

Sample Output

```
*A:7210-SAS># show system sync-if-timing
```

```
=====
System Interface Timing Operational Info
=====
```

```
System Status CPM A           : Master Locked
  Reference Input Mode         : Non-revertive
  Quality Level Selection      : Disabled
  System Quality Level         : unknown
```

```
Reference Order                : ref1 ref2
```

```
Reference Input 1
```

```
  Admin Status                 : up
  Rx Quality Level             : unknown
  Quality Level Override       : none
  Qualified For Use            : Yes
  Selected For Use             : Yes
  Source Port                  : 1/1/4
```

```
Reference Input 2
```

```
  Admin Status                 : up
  Rx Quality Level             : unknown
  Quality Level Override       : none
  Qualified For Use            : Yes
  Selected For Use             : No
  Not Selected Due To         : on standby
  Source Port                  : 1/1/6
```

```
=====
*A:7210-SAS>#
```

Sample output for 7210 SAS-D:

```
*7210-SASD># show system sync-if-timing
```

```
=====
System Interface Timing Operational Info
=====
```

```
System Status CPM A           : Master Locked
  Reference Input Mode         : Revertive
  Quality Level Selection      : Enabled
  System Quality Level         : prc
```

```
Reference Order                : ref1 ref2
```

```
Reference Input 1
```

```
  Admin Status                 : up
  Rx Quality Level             : prc
  Quality Level Override       : none
  Qualified For Use            : Yes
  Selected For Use             : Yes
  Source Port                  : 1/1/3
```

```
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                 : 1/1/5
=====
```

chassis

Syntax **chassis** [**environment**] [**power-supply**]

Context show

Description This command displays general chassis status information.

NOTE: The 'environment' option is supported only on 7210 SAS-E and 7210 SAS-D. The 'power-supply' option is supported only on 7210 SAS-D ETR.

Parameters *environment* — Displays chassis environmental status information.

Default Display all chassis information.

power-supply — Displays only power-supply information.

Chassis Output — The following table describes chassis output fields.

Label	Description
Name	The system name for the router.
Type	The router series model number.
Location	The system location for the device.
Coordinates	A user-configurable string that indicates the Global Positioning System (GPS) coordinates for the location of the chassis. For example: N 45 58 23, W 34 56 12 N37 37' 00 latitude, W122 22' 00 longitude N36*39.246' W121*40.121'
CLLI Code	The Common Language Location Identifier (CLLI) that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry.
Number of slots	The number of slots in this chassis that are available for plug-in cards. The total number includes card slots.
Number of ports	The total number of ports currently installed in this chassis.
Critical LED state	The current state of the Critical LED in this chassis.

Label	Description (Continued)
Major LED state	The current state of the Major LED in this chassis.
Minor LED state	The current state of the Minor LED in this chassis.
Base MAC address	The base chassis Ethernet MAC address.
Part number	The part number.
CLEI code	The code used to identify the router.
Serial number	The part number. Not user modifiable.
Manufacture date	The chassis manufacture date. Not user modifiable.
Manufacturing string	Factory-inputted manufacturing text string. Not user modifiable.
Time of last boot	The date and time the most recent boot occurred.
Current alarm state	Displays the alarm conditions for the specific board.
Number of fan trays	The total number of fan trays installed in this chassis.
Number of fans	The total number of fans installed in this chassis.
Operational status	Current status of the fan tray.
Fan speed	Half speed – The fans are operating at half speed. Full speed – The fans are operating at full speed.
Number of power supplies	The number of power supplies installed in the chassis.
Power supply number	The ID for each power supply installed in the chassis.
AC power	Within range – AC voltage is within range. Out of range – AC voltage is out of range.
DC power	Within range – DC voltage is within range. Out of range – DC voltage is out of range.
Over temp	Within range – The current temperature is within the acceptable range. Out of range – The current temperature is above the acceptable range.
Status	Up – The specified power supply is up.

Label	Description (Continued)
Down	— The specified power supply is down.

Sample Output

Note: This CLI output is obtained only if the hardware supports "DC source failure detection".

```
A:7210-SAS-E> show chassis
```

Chassis Information

```

Name                : STU2597
Type                : 7210 SAS-E-1
Location            :
Coordinates         :
CLLI code           :
Number of slots     : 2
Number of ports     : 24
Critical LED state   : Red
Major LED state     : Off
Minor LED state     : Off
Over Temperature state : OK
Base MAC address    : 00:25:ba:04:b9:bc

```

Hardware Data

```

Part number         : 3HE04410ABAC01
CLEI code           : IPMK310JRA
Serial number       : NS1026C0341
Manufacture date    : 06292010
Manufacturing string :
Manufacturing deviations :
Time of last boot   : 2010/11/09 16:12:40
Current alarm state : alarm active

```

Environment Information

```

Number of fan trays : 1
Number of fans      : 3

Fan tray number     : 1
Status              : up
Speed               : half speed

```

Power Supply Information

```

Number of power supplies : 2

Power supply number     : 1
Configured power supply type : dc
Status                  : failed
DC power                : out of range
Input power              : out of range

```

```

Output power           : within range

Power supply number    : 2
Configured power supply type : dc
Status                 : up
DC power               : within range
Input power            : within range
Output power           : within range

```

```

=====

A:7210-SAS-E>

```

```

A:7210-SAS-D> show chassis

```

```

=====
Chassis Information
=====

```

```

Name                  : 128sasdAc48v2573
Type                  : 7210 SAS-D 6F4T ETR-1
Location              :
Coordinates           :
CLLI code             :
Number of slots       : 2
Number of ports       : 10
Critical LED state    : Off
Major LED state       : Off
Minor LED state       : Off
Over Temperature state : OK
Low Temperature state : OK
Base MAC address      : 4c:5f:d2:07:39:d0

```

```

Hardware Data

```

```

Part number           : 3HE05676ADAA01
CLEI code             : IPMSX10BRA
Serial number         : NS1139C0070
Manufacture date      : 09242011
Manufacturing string   :
Manufacturing deviations :
Time of last boot     : 2012/04/19 10:44:51
Current alarm state    : alarm active

```

```

-----
Power Supply Information

```

```

Number of power supplies : 2

Power supply number      : 1
Configured power supply type : dc (-48V)
Status                   : up

Power supply number      : 2
Status                   : failed
Configured power supply type : ac

```

```

=====

A:7210-SAS-D>

```

```

A:7210SAS>show# chassis power-supply

```

```
Chassis Information
=====
Power Supply Information
  Number of power supplies      : 2

  Power supply number          : 1
  Configured power supply type  : dc (-48V)
  Status                       : up

  Power supply number          : 2
  Status                       : failed
  Configured power supply type  : ac
=====
A:7210SAS>show#
```

Output for Chassis Environment.

```
*A:SASE>show# chassis environment

=====
Chassis Information
=====
Environment Information
  Number of fan trays          : 1
  Number of fans               : 3

  Fan tray number             : 1
  Status                      : up
  Speed                       : half speed
=====
*A:SASE>show#
```

Output for older 7210 SAS-E devices without input-fail-detection)

```
*A:7210-SAS-E# show chassis power-supply
=====
Chassis Information
=====
Power Supply Information
  Number of power supplies      : 2
  Power supply number          : 1
  Defaulted power supply type  : none
  Status                       : not equipped
  Power supply number          : 2
  Configured power supply type  : dc (+24V)
  Status                       : up
=====
*A:7210-SAS-E#

*A:7210-SAS-E# show chassis power-supply
=====
Chassis Information
=====
Power Supply Information
  Number of power supplies      : 2
  Power supply number          : 1
  Configured power supply type  : ac single
```



```

Status                : up
AC power               : within range
Power supply number    : 2
Configured power supply type : dc (-48V)
Status                : up
=====
*A:7210-SAS-E#

*A:7210-SAS-E# show chassis power-supply
=====
Chassis Information
=====
Power Supply Information
  Number of power supplies      : 2
  Power supply number          : 1
  Configured power supply type  : dc (+48V)
  Status                      : up
  DC power                    : within range
  Input power                 : within range
  Output power                : within range
  Power supply number          : 2
  Configured power supply type  : dc (+24V)
  Status                      : failed
  DC power                    : out of range
  Input power                 : out of range
  Output power                : within range
=====
*A:7210-SAS-E#

```

alarm-contact-input

NOTE: This command is supported only on 7210 SAS-E devices.

- Syntax** **alarm- contact-input all**
alarm-contact-input <*alarm-contact-input-id*> [detail]
- Context** show>alarm-contact
- Description** This command displays information of all the alarm contact input pins.
- Output** **alarm-contact-input Output** — The following table describes alarm-contact-input output fields.

Label	Description
Alarm input pin Number	Indicates the pin alarm input pin number.
Alarm input pin Description	Describes the alarm indicating its usage or attribute.
Alarm input pin current state	Indicates the current state of the alarm contact input pin.

Label	Description (Continued)
Alarm output pin used	Indicates the alarm output pin used.
Last state change time	Indicates the previous state change time.

Sample Output

```
*A:7210-2# show alarm-contact-input 1
=====
Alarm Contact Input
=====
    Alarm Input Pin Number      : 1
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
=====
*A:7210-2#

*A:7210-2# show alarm-contact-input 1 detail
=====
Alarm Contact Input
=====
    Alarm Input Pin Number      : 1
    Alarm Input Pin Description :
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
    Last State Change           : 05/19/2010 11:28:09
=====
*A:7210-2#

*A:7210-2# show alarm-contact-input all
=====
Alarm Contact Input
=====
    Alarm Input Pin Number      : 1
    Alarm Input Pin Description :
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
    Last State Change           : 05/19/2010 11:28:09
    Alarm Input Pin Number      : 2
    Alarm Input Pin Description :
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
    Last State Change           : 05/19/2010 11:28:09
    Alarm Input Pin Number      : 3
    Alarm Input Pin Description :
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
    Last State Change           : 05/19/2010 11:28:09
    Alarm Input Pin Number      : 4
    Alarm Input Pin Description :
    Alarm Input Pin Current State : Disabled
    Alarm Output Pin Used       : Major
    Last State Change           : 05/19/2010 11:28:09
=====
```

*A:7210-2#

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} no force-reference
Context	debug>sync-if-timing
Description	This command allows an operator to force the system synchronous timing output to use a specific reference. Note: This command should be used for testing and debugging purposes only. Once the system timing reference input has been forced, it will not revert back to another reference at anytime. The state of this command is not persistent between system boots. When the debug force-reference command is executed, the current system synchronous timing output is immediately referenced from the specified reference input. If the specified input is not available (shutdown), or in a disqualified state, the timing output will enter the holdover state based on the previous input reference.
Parameters	ref1 — The clock will use the first timing reference. ref2 — The clock will use the second timing reference.

system

Syntax	[no] system
Context	debug
Description	This command displays system debug information.

ntp

Syntax	[no] router <i>router-name</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-name</i> — Base 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.

Clear Commands

completed

Syntax	completed [<i>action-name</i>] [owner <i>action-owner</i>]
Context	clear>cron>action
Description	This command clears completed CRON action run history entries.
Parameters	<i>action-name</i> — Specifies the action name. Values maximum 32 characters <i>owner</i> <i>action-owner</i> — Specifies the owner name. Default TiMOS CLI

screen

Syntax	screen
Context	clear
Description	This command allows an operator to clear the Telnet or console screen.

sync-if-timing

Syntax	sync-if-timing { <i>ref1</i> <i>ref2</i> }
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	<i>ref1</i> — clears the first timing reference <i>ref2</i> — clears the second timing reference

FAN CONTROLLER DEBUG COMMANDS

fan-stats

Syntax	fan-stats
Context	tools>dump
Description	This command provides details of the fan operation.

Sample Output

The following table describes fan-stats output fields.

Label	Description
Fan Configuration Mode	Displays the user configured mode for fan operation. It can be On/Off/Auto.
Fan Status	Displays the current status of the fan. It can be On / Off.
Auto Mode Duration	Displays the total duration since the fan has been in auto mode. Displayed in HH:MM format to indicate hours and minutes. Valid only when the Fan configuration mode is auto.
Fan ON count	Displays the total number of times the Fan has been switched 'ON' in auto mode. Valid only in auto mode.

```
A:7210SAS# tools dump system fan-stats
```

```
Fan Configuration Mode : Auto
Fan Status : Off
Auto Mode Duration : 70 hr:24 min
Fan ON Count : 2
```

NOTE: When the fan mode is changed by the user, the values displayed above are automatically reset by the software.

Standards and Protocol Support (7210 SAS-D)

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)
Protocol Support

DHCP

RFC 2131 Dynamic Host Configuration Protocol
RFC 3046 DHCP Relay Agent Information Option (Option 82)

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function

M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASED-ACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 SNMP MIB draft-ietf-disman-alarm-mib-04.txt
RFC 3418 SNMP MIB
Efficient Handling of in-Profile Traffic [Only for 7210 SAS-D]
IPv6 [Only for 7210 SAS-E]

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

IPv6

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Auto configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 3587 IPv6 Global Unicast Address Format
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1

RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASED-ACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-disman-alarm-mib-04.txt
RFC 3418 SNMP MIB

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol

draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option

Timing (Only on 7210 SAS-D ETR)

ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.
GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005
ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.
ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.
ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-E-V5v0.mib (Only for 7210 SAS-E)
TIMETRA-CAPABILITY-7210-SAS-D-V5v0.mib (Only for 7210 SAS-D)
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-MIB.mib [Only for 7210 SAS-E]
TIMETRA-SAS-FILTER-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-LOG-MIB.mib
TIMETRA-SAS-MIRROR-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib

Standards and Protocol Support (7210 SAS E)

Standards Compliance

IEEE 802.1ab-REV/D3 Station And Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 1)

Protocol Support

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP

RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASED-ACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 SNMP MIB draft-ietf-disman-alarm-mib-04.txt
RFC 3418 SNMP MIB

IPv6

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Auto configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 3587 IPv6 Global Unicast Address Format
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

MULTICAST

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol

Standards and Protocols

draft-ietf-secsh-connection.txt SSH
Connection Protocol
draft-ietf-secsh-newmodes.txt SSH
Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

NETWORK MANAGEMENT

ITU-T X.721: Information technology-
OSI-Structure of Management
Information
ITU-T X.734: Information technology-
OSI-Systems Management: Event
Report Management Function
M.3100/3120 Equipment and Connection
Models
TMF 509/613 Network Connectivity
Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining
Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-
NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-
SMMIB
RFC 2575 SNMP-VIEW-BASED-ACM-
MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for
Describing Simple Network
Management Protocol (SNMP)
Management Frameworks
RFC 3412 - Message Processing and
Dispatching for the Simple Network
Management Protocol (SNMP)

RFC 3413 - Simple Network
Management Protocol (SNMP)
Applications
RFC 3414 - User-based Security Model
(USM) for version 3 of the Simple
Network Management Protocol
(SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-disman-alarm-mib-04.txt

PROPRIETARY MIBs

ALCATEL-IGMP-SNOOPING-
MIB.mib
TIMETRA-CAPABILITY-7210-SAS-E-
V5v0.mib (Only for 7210 SAS-E)
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-
MIB.mib [Only for 7210 SAS-E]
TIMETRA-SAS-FILTER-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-
MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-LOG-MIB.mib.mib
TIMETRA-SAS-MIRROR-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib

INDEX

A

auto mode 112

B

BOF

overview

image loading

persistence 119

saving a configuration 142

configuring

accessing

the CLI 137

console connection 137

basic 131

BOF parameters 139

command reference 147

management tasks 140

overview 130

rebooting 145

searching for BOF file 134

C

CLI

usage

basic commands 22

command prompt 29

displaying context configurations 30, 27

entering CLI commands 34, 25, 33

monitor commands 26

navigating 20

structure 18

F

File system

overview

compact flash devices 82

URLs 84

configuring 87

command reference 93, 89, 88

displaying information 91

moving files 90

removing/deleting 90

I

image loading 114

L

lldp 270

M

manual mode 111

S

System

overview

backup config files 240

CLLI 176

contact 174, 175

location 175

name 174

saving configurations 203, 212

time 177

configuring

basic 213

command reference

administration commands 267

synchronization commands 269, 261,
264, 265

revert 252

system administration parameters 241,
215, 219

timing 250

