



Alcatel-Lucent

Service Access Switch | Release 8.0 Rev.06

7210 SAS M, T, X, R6, R12, Mxp, Sx OS
System Management Guide

3HE10387AAADTQZZA



Alcatel-Lucent - Proprietary & Confidential

Contains proprietary/trade secret information which is the property of Alcatel-Lucent. Not to be made available to, or copied or used by anyone who is not an employee of Alcatel-Lucent except when there is a valid nondisclosure agreement in place which covers such information and contains appropriate non-disclosure and limited use obligations.

Copyright 2015 © Alcatel-Lucent. All rights reserved. All specifications, procedures, and information in this document are subject to change and revision at any time without notice. The information contained herein is believed to be accurate as of the date of publication. AlcatelLucent



All specifications, procedures, and information in this document are subject to change and revision at any time without notice. The information contained herein is believed to be accurate as of the date of publication. Alcatel-Lucent provides no warranty, express or implied, regarding its contents. Users are fully responsible for application or use of the documentation.

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2015 Alcatel-Lucent.

All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

TABLE OF CONTENTS

Preface	11
Getting Started	
Alcatel-Lucent 7210 SAS Router Configuration Process	15
Security	
Authentication, Authorization, and Accounting	18
Authentication	19
Local Authentication	20
RADIUS Authentication	20
TACACS+ Authentication	23
Authorization	24
Local Authorization	25
RADIUS Authorization	25
TACACS+ Authorization	25
Accounting	26
RADIUS Accounting	26
TACACS+ Accounting	26
Security Controls	28
When a Server Does Not Respond	28
Access Request Flow	29
Vendor-Specific Attributes (VSAs)	30
Sample User (VSA) Configuration	33
Alcatel-Lucent Dictionary	34
Other Security Features	37
Secure Shell (SSH)	37
Exponential Login Backoff	39
User Lockout	40
Encryption	41
802.1x Network Access Control	41
TCP Enhanced Authentication Option	41
Packet Formats	42
Keychain	44
Configuration Notes	45
General	45
Configuring Security with CLI	47
Setting Up Security Attributes	48
Configuring Authentication	48
Configuring Authorization	49
Configuring Accounting	51
Security Configurations	52
Configuration Tasks	54
Security Configuration Procedures	55
Configuring Management Access Filters	55
Configuring Password Management Parameters	56

Table of Contents

Configuring Profiles	57
Configuring Users	58
Configuring Keychains	59
Copying and Overwriting Users and Profiles	60
User	60
Profile	62
RADIUS Configurations	64
Configuring RADIUS Authentication	64
Configuring RADIUS Authorization	65
Configuring RADIUS Accounting	66
Configuring 802.1x RADIUS Policies	67
TACACS+ Configurations	67
Enabling TACACS+ Authentication	67
Configuring TACACS+ Authorization	69
Configuring TACACS+ Accounting	70
Enabling SSH	71
Configuring Login Controls	72
Security Command Reference	73
Command Hierarchies	73
Configuration Commands	73

SNMP

SNMP Overview	162
SNMP Architecture	162
Management Information Base	162
SNMP Protocol Operations	163
SNMP Versions	163
Management Information Access Control	164
User-Based Security Model Community Strings	165
Views	165
Access Groups	165
Users	166
Which SNMP Version to Use?	167
Configuration Notes	169
General	169
Configuring SNMP with CLI	171
SNMP Configuration Overview	172
Configuring SNMPv1 and SNMPv2c	172
Configuring SNMPv3	172
Basic SNMP Security Configuration	173
Configuring SNMP Components	174
Configuring a Community String	175
Configuring View Options	176
Configuring Access Options	177
Configuring USM Community Options	179
Configuring Other SNMP Parameters	180
SNMP Command Reference	181
Command Hierarchies	181
Configuration Commands	181

Event and Accounting Logs

Logging Overview	212
Log Destinations	214
Console	214
Session	214
Memory Logs	214
Log Files	215
SNMP Trap Group	217
Syslog	217
Event Logs	219
Event Sources	220
Event Control	222
Log Manager and Event Logs	224
Event Filter Policies	225
Event Log Entries	226
Simple Logger Event Throttling	228
Default System Log	229
Accounting Logs	230
Accounting Records	230
Configuration Guidelines	268
Accounting Files	269
Design Considerations	269
Configuration Notes	270
Configuring Logging with CLI	271
Log Configuration Overview	272
Log Types	272
Basic Event Log Configuration	273
Common Configuration Tasks	274
Configuring an Event Log	274
Configuring a File ID	276
Configuring an Accounting Policy	277
Configuring Event Control	278
Configuring Throttle Rate	279
Configuring a Log Filter	280
Configuring an SNMP Trap Group	281
Configuring a Syslog Target	282
Log Management Tasks	283
Modifying a Log File	284
Deleting a Log File	286
Modifying a File ID	287
Deleting a File ID	289
Modifying a Syslog ID	290
Deleting a Syslog	291
Modifying an SNMP Trap Group	292
Deleting an SNMP Trap Group	293
Modifying a Log Filter	294
Deleting a Log Filter	296
Modifying Event Control Parameters	297
Returning to the Default Event Control Configuration	298

Table of Contents

Configuring SNMP Dying Gasp	298
Configuration Guidelines for SNMP Dying Gasp Trap	300
Log Command Reference	301
Command Hierarchies	301
Facility Alarms	
Facility Alarms Overview	378
Facility Alarms vs. Log Events	379
Facility Alarm Severities and Alarm LED Behavior	381
Facility Alarm Hierarchy	382
Facility Alarm List	383
Configuring Logging with CLI	387
Basic Facility Alarm Configuration	388
Common Configuration Tasks	389
Configuring the Maximum Number of Alarms To Clear	389
Facility Alarms Command Reference	391
Command Hierarchies	391
Standards and Protocol Support	397
Index	403

LIST OF TABLES

Getting Started

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

Security

Table 2:	Supported Authorization Configurations	24
Table 3:	Security Methods Capabilities	28
Table 4:	Keychain Mapping	44
Table 5:	Security Configuration Requirements	54
Table 6:	Show System Security Access Group Output Fields	141
Table 7:	Show System Security Authentication Output Fields	142
Table 8:	Show Communities Output Fields	144
Table 9:	Show Management Access Filter Output Fields	146
Table 10:	Show Management Access Filter Output Fields	148
Table 11:	Show Management Access Filter Output Fields	149
Table 12:	Show User Profile Output Fields	150
Table 13:	Show Source Address Output Fields	152
Table 14:	Show View Output Fields	156
Table 15:	Show Users Output Fields	158

SNMP

Table 16:	Counters Output Fields	193
Table 17:	Show System Information Output Fields	194
Table 18:	Show System Information Output Fields	198
Table 19:	Show Communities Output Fields	201
Table 20:	Show Management Access Filter Output Fields	202
Table 21:	Show SSH Output Fields	207
Table 22:	Show User Output Fields	208
Table 23:	Show System Security View Output Fields	209

Event and Accounting Logs

Table 24:	Event Severity Levels	212
Table 25:	7210 SAS-Series to Syslog Severity Level Mappings	218
Table 26:	Valid Filter Policy Operators	225
Table 27:	Log Entry Field Descriptions	226
Table 28:	Accounting Record Names and Collection Periods	230
Table 29:	Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode)	234
Table 30:	Accounting Record Name Details for 7210 SAS-X	243
Table 31:	Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12	252
Table 32:	Accounting Record Name Details for 7210 SAS-Mxp	261
Table 34:	Show Accounting Policy Output Fields	347
Table 35:	Accounting Policy Output Fields	349
Table 36:	Event Log Filter Summary Output Fields	365
Table 37:	Event Log Filter Detail Output Fields	366
Table 38:	Log Filter Match Criteria Output Fields	366
Table 39:	Show Log-Collector Output Fields	368

List of Tables

Table 40:	SNMP Trap Group Output Fields	373
Table 41:	Show Log Syslog Output Fields	374

Facility Alarms

Table 42:	Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event	383
Table 43:	Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event	383
Table 44:	linkDown Facility Alarm Support	386
Table 45:	Show Facility Alarms Output Fields	395

LIST OF FIGURES

Security

Figure 1:	RADIUS Requests and Responses	18
Figure 2:	Security Flow	29

SNMP

Figure 3:	SNMPv1 and SNMPv2c Configuration and Implementation Flow	168
-----------	--	-----

Event and Accounting Logs

Figure 4:	Event Logging Block Diagram	219
Figure 5:	Show Log Applications Command Output	221

Facility Alarms

Figure 6:	Log Events, Alarms and LEDs	379
-----------	-----------------------------------	-----

About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure 7210 SAS-M, T, X, R6, R12, Mxp, Sx boot option file (BOF), file system and system management functions.

On 7210 SAS devices, not all the CLI commands are supported on all the platforms and in all the modes. In many cases, the CLI commands are mentioned explicitly in this document. In other cases, it is implied and easy to know the CLIs that are not supported on a particular platform.

All the variants of 7210 SAS-M and 7210 SAS-T can be configured in two modes, that is in network mode and in access-uplink mode. In network mode configuration 7210 SAS-M and 7210 SAS-T uses IP/MPLS to provide service transport. In access-uplink mode configuration 7210 SAS-M and 7210 SAS-T uses Ethernet QinQ technology to provide service transport. The mode can be selected by configuring the BOF appropriately. The 7210 SAS-Mxp and 7210 SAS-Sx can only be configured in Network mode. It does not support access-uplink mode.

7210 SAS-Sx can be operated in standalone mode and satellite mode. The user guide provides features and CLI commands supported in 7210 SAS-Sx standalone mode of operations. Only the Basic System Configuration User Guide contains information on how to boot the 7210 SAS-Sx in satellite mode of operation.

This guide also presents examples to configure and implement various tests.

Notes:

- This user guide is applicable to all 7210 SAS-M, 7210 SAS-T, 7210 SAS-X, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Mxp, and 7210 SAS-Sx platforms, unless specified otherwise.
- In either mode, it is expected that the user will only configure the required CLI parameters appropriate for the mode he intends to use. Unless otherwise noted, most of the configuration is similar in both the network mode and Access uplink mode.
- Only 7210 SAS-M and 7210 SAS-T supports access-uplink mode. 7210 SAS-X, 7210 SAS-R6 and 7210 SAS-R12 does not support access-uplink mode. 7210 SAS-X, 7210

SAS-R6 and 7210 SAS-R12 supports only MPLS uplinks and implicitly operates in network mode. The 7210 SAS-Mxp supports only network mode.

- On 7210 SAS devices, not all the CLI commands are supported on all the platforms and in all the modes. In many cases, the CLI commands are mentioned explicitly in this document. In other cases, it is implied and easy to know the CLIs that are not supported on a particular platform.

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 CLLI code, time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), and synchronization properties

List of Technical Publications

The 7210 SAS M, T, X, R6, R12, Mxp, Sx OS documentation set is composed of the following books:

- 7210 SAS M, T, X, R6, R12, Mxp, Sx OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7210 SAS M, T, X, R6, R12, Mxp, Sx OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7210 SAS M, T, X, R6, R12, Mxp, Sx OS Interface Configuration Guide
This guide describes card, Media Dependent Adapter (MDA), link aggregation group (LAG) and port provisioning.
- 7210 SAS M, T, X, R6, R12, Mxp, Sx OS Router Configuration Guide
This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, as well as IP-based filtering.
- 7210 SAS M, T, X, R6, R12, Mxp, Sx OS Routing Protocols Guide
This guide provides an overview of routing concepts and provides configuration examples for protocols and route policies.
- 7210 SAS-M, T, Mxp, Sx OS and 7210 SAS-X, R6, R12 OS Services Guide
This guide describes how to configure service parameters such as customer information, and user services.
- 7210 SAS M, T, X, R6, R12, Mxp, Sx 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-M, T, Mxp, Sx and 7210 SAS-X, R6, R12 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 device and related products from a distributor or authorized re-seller, contact the technical support staff for that distributor or re-seller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center:

Web: <http://www.alcatel-lucent.com/wps/portal/support>

Getting Started

In This Chapter

This chapter provides process flow information to configure system security and access functions as well as event and accounting logs.

Alcatel-Lucent 7210 SAS Router Configuration Process

[Table 1](#) lists the tasks necessary to configure system security and access functions and logging features. Each chapter in this book is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

Area	Task	Chapter
System security	Configure system security parameters, such as authentication, authorization, and accounting.	Security on page 17
Network management	Configure SNMP elements.	SNMP on page 161
Operational functions	Configure event and accounting logs.	Event and Accounting Logs on page 211
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 397

In This Chapter

This chapter provides information to configure security parameters. Topics in this chapter include:

- [Authentication, Authorization, and Accounting on page 18](#)
 - [Authentication on page 19](#)
 - [Authorization on page 24](#)
 - [Accounting on page 26](#)
- [Security Controls on page 28](#)
 - [When a Server Does Not Respond on page 28](#)
 - [Access Request Flow on page 29](#)
- [Vendor-Specific Attributes \(VSAs\) on page 30](#)
- [Other Security Features on page 37](#)
 - [Secure Shell \(SSH\) on page 37](#)
 - [Encryption on page 41](#)
- [Configuration Notes on page 45](#)

Authentication, Authorization, and Accounting

This chapter describes authentication, authorization, and accounting (AAA) used to monitor and control network access on 7210 SAS routers. Network security is based on a multi-step process. The first step, authentication, validates a user's name and password. The second step is authorization, which allows the user to access and execute commands at various command levels based on profiles assigned to the user.

Another step, accounting, keeps track of the activity of a user who has accessed the network. The type of accounting information recorded can include a history of the commands executed, the amount of time spent in the session, the services accessed, and the data transfer size during the session. The accounting data can then be used to analyze trends, and also for billing and auditing purposes.

You can configure 7210 SAS routers to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, or FTP. You can select the authentication order which determines the authentication method to try first, second, and third.

7210 SAS supports the following security features:

- RADIUS can be used for authentication, authorization, and accounting.
- TACACS+ can be used for authentication, authorization, and accounting.
- Local security can be implemented for authentication and authorization.

Figure 1 depicts end user access-requests sent to a RADIUS server. After validating the user names and passwords, the RADIUS server returns an access-accept message to the users on ALA-1 and ALA-2. The user name and password from ALA-3 could not be authenticated, thus access was denied.

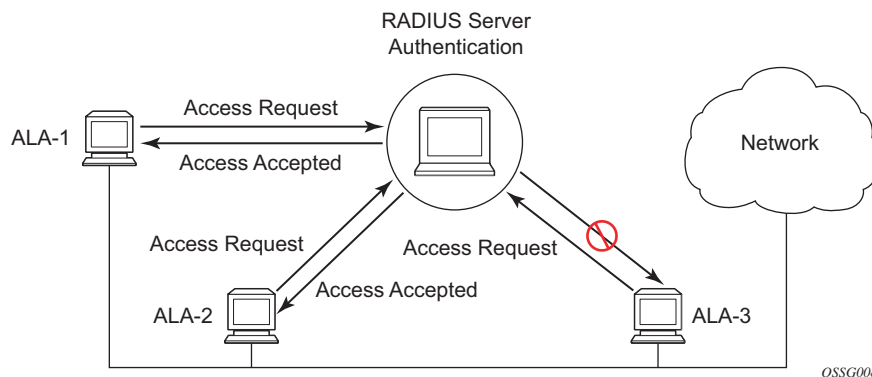


Figure 1: RADIUS Requests and Responses

Authentication

Authentication validates a user name and password combination when a user attempts to log in.

When a user attempts to log in through the console, Telnet, SSH, SCP, or FTP, the 7210 SAS-Series client sends an access request to a RADIUS, TACACS+, or local database.

Transactions between the client and a RADIUS server are authenticated through the use of a shared secret. The secret is never transmitted over the network. User passwords are sent encrypted between the client and RADIUS server which prevents someone snooping on an insecure network to learn password information.

If the RADIUS server does not respond within a specified time, the router issues the access request to the next configured servers. Each RADIUS server must be configured identically to guarantee consistent results.

If any RADIUS server rejects the authentication request, it sends an access reject message to the router. In this case, no access request is issued to any other RADIUS servers. However, if other authentication methods such as TACACS+ and/or local are configured, then these methods are attempted. If no other authentication methods are configured, or all methods reject the authentication request, then access is denied.

For the RADIUS server selection, round-robin is used if multiple RADIUS servers are configured. Although, if the first alive server in the list cannot find a user-name, the router does not re-query the next server in the RADIUS server list and denies the access request. It may get authenticated on the next login attempt if the next selected RADIUS server has the appropriate user-name. It is recommended that the same user databases are maintained for RADIUS servers in order to avoid inconsistent behavior.

The user login is successful when the RADIUS server accepts the authentication request and responds to the router with an access accept message.

Implementing authentication without authorization for the 7210 SAS-Series routers does not require the configuration of VSAs (Vendor Specific Attributes) on the RADIUS server. However, users, user access permissions, and command authorization profiles must be configured on each router.

Any combination of these authentication methods can be configured to control network access from a 7210 SAS-Series router:

- [Local Authentication on page 20](#)
- [RADIUS Authentication on page 20](#)
- [TACACS+ Authentication on page 23](#)

Local Authentication

Local authentication uses user names and passwords to authenticate login attempts. The user names and passwords are local to each router not to user profiles.

By default, local authentication is enabled. When one or more of the other security methods are enabled, local authentication is disabled. Local authentication is restored when the other authentication methods are disabled. Local authentication is attempted if the other authentication methods fail and local is included in the authentication order password parameters.

Locally, you can configure user names and password management information. This is referred to as local authentication. Remote security servers such as RADIUS or TACACS+, are not enabled.

RADIUS Authentication

Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize access to the requested system or service.

RADIUS allows you to maintain user profiles in a shared central database and provides better security, allowing a company to set up a policy that can be applied at a single administered network point.

RADIUS Server Selection

The RADIUS server selection algorithm is used by different applications:

- RADIUS operator management
- RADIUS authentication for Enhanced Subscriber Management
- RADIUS accounting for Enhanced Subscriber Management
- RADIUS PE-discovery

In all these applications, up to 5 RADIUS servers pools (per RADIUS policy, if used) can be configured.

The RADIUS server selection algorithm can work in 2 modes, either Direct mode or Round-robin mode.

Direct Mode

The first server is used as the primary server. If this server is unreachable, the next server, based on the server index, of the server pool is used. This continues until either all servers in the pool have been tried or an answer is received.

If a server is unreachable, it will not be used again by the RADIUS application for the next 30 seconds to allow the server to recover from its unreachable state. After 30 seconds the unreachable server is available again for the RADIUS application. If in these 30 seconds the RADIUS application receives a valid response for a previously sent RADIUS packet on that unreachable server, the server will be available for the RADIUS application again, immediately after reception of that response.

Round-Robin Mode

The RADIUS application sends the next RADIUS packet to the next server in the server pool. The same server non-reachability behavior is valid as in the Direct mode.

Server Reachability Detection

A server is reachable, when the operational state UP, when a valid response is received within a timeout period which is configurable by the retry parameter on the RADIUS policy level.

A server is treated as not-reachable, when the operational state down, when the following occurs:

- A timeout — If a number of consecutive timeouts are encountered for a specific server. This number is configurable by the retry parameter on RADIUS policy level.
- A send failed — If a packet cannot be sent to the RADIUS server because the forwarding path towards the RADIUS server is broken (for example, the route is not available, the interface shutdown, etc.), then, no retry mechanism is invoked and immediately, the next server in line is used.

A server that is down can only be used again by the RADIUS algorithm after 30 seconds, unless, during these 30 seconds a valid RADIUS reply is received for that server. Then, the server is immediately marked UP again.

The operational state of a server can also be “unknown” if the RADIUS application is not aware of the state of the RADIUS server (for example, if the server was previously down but no requests had been sent to the server, thus, it is not certain yet whether the server is actually reachable).

Application Specific Behavior

Operator Management

The server access mode is fixed to Round-Robin (Direct cannot be configured for operator management). A health-check function is available for operator management, which can optionally be disabled. The health-check polls the server once every 10 seconds with an improbable user name. If the server does not respond to this health-check, it will be marked down.

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

RADIUS Authentication

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

RADIUS Accounting

The RADIUS accounting application will try to send all the concerned packets of a subscriber host to the same server. If that server is down, then the packet is sent to the next server and, from that moment on, the RADIUS application uses that server to send its packets for that subscriber host.

RADIUS PE-Discovery

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

The RADIUS PE-discovery application makes use of a 10 second time period instead of the generic 30 seconds and uses a fixed consecutive timeout value of 2 (see [Server Reachability Detection on page 21](#)).

As long as the Session-Timeout (attribute in the RADIUS user file) is specified, it is used for the polling interval. Otherwise, the configured polling interval will be used (60 seconds by default).

TACACS+ Authentication

Terminal Access Controller Access Control System, commonly referred to as TACACS is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol and therefore less secure than the later Terminal Access Controller Access Control System Plus (TACACS+) and RADIUS protocols.

TACACS+ and RADIUS have largely replaced earlier protocols in the newer or recently updated networks. TACACS+ uses Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). TACACS+ is popular as TCP is thought to be a more reliable protocol. RADIUS combines authentication and authorization. TACACS+ separates these operations.

Authorization

The OS support local, RADIUS, and TACACS+ authorization to control the actions of specific users by applying a profile based on user name and password configurations once network access is granted. The profiles are configured locally as well as VSAs on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 30](#).

Once a user has been authenticated using RADIUS (or another method), the router can be configured to perform authorization. The RADIUS server can be used to:

- Download the user profile to the router
- Send the profile name that the node should apply to the router.

Profiles consist of a suite of commands that the user is allowed or not allowed to execute. When a user issues a command, the authorization server looks at the command and the user information and compares it with the commands in the profile. If the user is authorized to issue the command, the command is executed. If the user is not authorized to issue the command, then the command is not executed.

Profiles must be created on each router and should be identical for consistent results. If the profile is not present, then access is denied.

[Table 2](#) displays the following scenarios:

- Remote (RADIUS) authorization cannot be performed if authentication is done locally (on the router).
- The reverse scenario is supported if RADIUS authentication is successful and no authorization is configured for the user on the RADIUS server, then local (router) authorization is attempted, if configured in the authorization order.

When authorization is configured and profiles are downloaded to the router from the RADIUS server, the profiles are considered temporary configurations and are not saved when the user session terminates.

Table 2: Supported Authorization Configurations

	RADIUS Supplied Profile
Configured user	Not Supported
RADIUS server configured user	Supported
TACACS+ server configured user	Not Supported

When using authorization, maintaining a user database on the router is not required. User names can be configured on the RADIUS server. User names are temporary and are not saved in the configuration when the user session terminates. Temporary user login names and their associated passwords are not saved as part of the configuration.

- [Local Authorization on page 25](#)
 - [RADIUS Authorization on page 25](#)
 - [TACACS+ Authorization on page 25](#)
-

Local Authorization

Local authorization uses user profiles and user access information after a user is authenticated. The profiles and user access information specifies the actions the user can and cannot perform.

By default, local authorization is enabled. Local authorization is disabled only when a different remote authorization method is configured (RADIUS authorization). Local authorization is restored when RADIUS authorization is disabled.

You must configure profile and user access information locally.

RADIUS Authorization

RADIUS authorization grants or denies access permissions for a router. Permissions include the use of FTP, Telnet, SSH (SCP), and console access. When granting Telnet, SSH (SCP) and console access to the router, authorization can be used to limit what CLI commands the user is allowed to issue and which file systems the user is allowed or denied access.

TACACS+ Authorization

Like RADIUS authorization, TACACS+ grants or denies access permissions for a router. The TACACS+ server sends a response based on the username and password.

TACACS+ separates the authentication, authorization, and accounting function. RADIUS combines the authentication and authorization functions.

Accounting

When enabled, RADIUS accounting sends command line accounting from the router to the RADIUS server. The router sends accounting records using UDP packets at port 1813 (decimal).

The router issues an accounting request packet for each event requiring the activity to be recorded by the RADIUS server. The RADIUS server acknowledges each accounting request by sending an accounting response after it has processed the accounting request. If no response is received in the time defined in the timeout parameter, the accounting request must be retransmitted until the configured retry count is exhausted. A trap is issued to alert the NMS (or trap receiver) that the server is unresponsive. The router issues the accounting request to the next configured RADIUS server (up to 5).

User passwords and authentication keys of any type are never transmitted as part of the accounting request.

RADIUS Accounting

Accounting tracks user activity to a specified host. When RADIUS accounting is enabled, the server is responsible for receiving accounting requests and returning a response to the client indicating that it has successfully received the request. Each command issued on the router generates a record sent to the RADIUS server. The record identifies the user who issued the command and the timestamp.

Accounting can be configured independently from RADIUS authorization and RADIUS authentication.

TACACS+ Accounting

The OS allows you to configure the type of accounting record packet that is to be sent to the TACACS+ server when specified events occur on the device. The accounting **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent. Start/stop messages are only sent for individual commands, not for the session.

When a user logs in to request access to the network using Telnet or SSH, or a user enters a command for which accounting parameters are configured, or a system event occurs, such as a reboot or a configuration file reload, the router checks the configuration to see if TACACS+ accounting is required for the particular event.

If TACACS+ accounting is required, then, depending on the accounting record type specified, sends a start packet to the TACACS+ accounting server which contains information about the event.

The TACACS+ accounting server acknowledges the start packet and records information about the event. When the event ends, the device sends a stop packet. The stop packet is acknowledged by the TACACS+ accounting server.

Security Controls

You can configure routers to use RADIUS, TACACS+, and local authentication to validate users requesting access to the network. The order in which password authentication is processed among RADIUS, TACACS+ and local passwords can be specifically configured. In other words, the authentication order can be configured to process authorization through TACACS+ first, then RADIUS for authentication and accounting. Local access can be specified next in the authentication order in the event that the RADIUS and TACACS+ servers are not operational.

Table 3: Security Methods Capabilities

Method	Authentication	Authorization	Accounting*
Local	Y	Y	N
TACACS+	Y	Y	Y
RADIUS	Y	Y	Y

* Local commands always perform account logging using the **config log** command.

When a Server Does Not Respond

A trap is issued if a RADIUS + server is unresponsive. An alarm is raised if RADIUS is enabled with at least one RADIUS server and no response is received to either accounting or user access requests from any server.

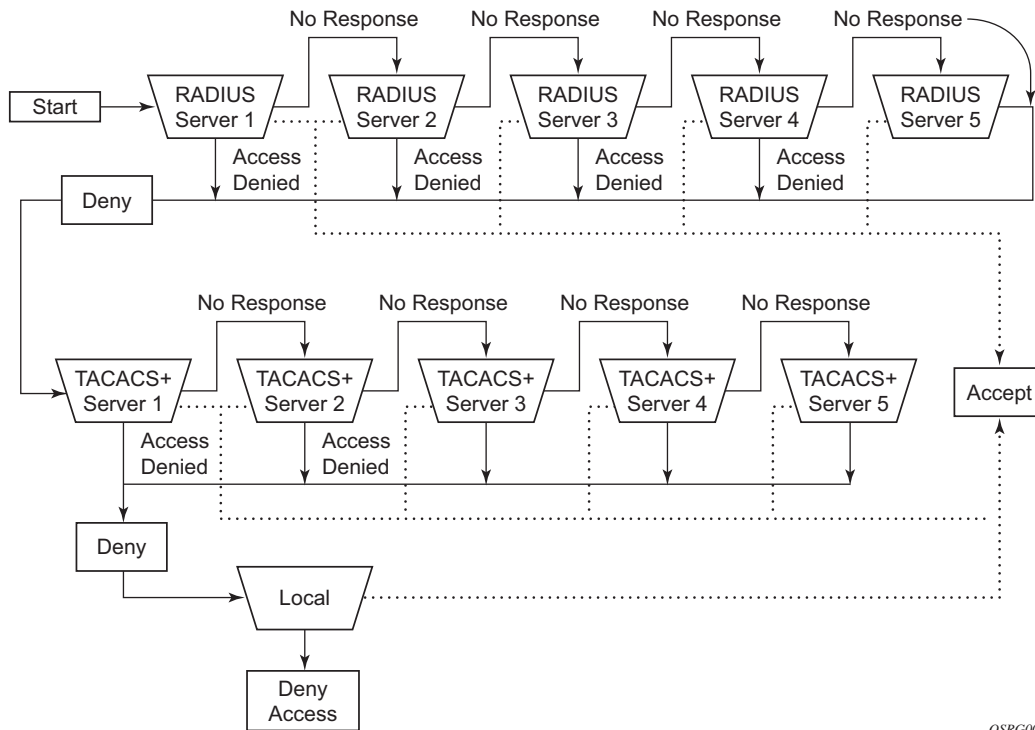
Periodic checks to determine if the primary server is responsive again are not performed. If a server is down, it will not be contacted for 5 minutes. If a login is attempted after 5 minutes, then the server is contacted again. When a server does not respond with the health check feature enabled, the server's status is checked every 30 seconds. Health check is enabled by default. When a service response is restored from at least one server, the alarm condition is cleared. Alarms are raised and cleared on Alcatel-Lucent's Fault Manager or other third party fault management servers.

The servers are accessed in order from lowest to highest specified index (from 1 to 5) for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received, implying a lower indexed server is not available. If a response from the server is received, no other server is queried.

Access Request Flow

In [Figure 2](#), the authentication process is defined in the `config>system>security>password` context. The authentication order is determined by specifying the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords. This example uses the authentication order of RADIUS, then TACACS+, and finally, local. An access request is sent to RADIUS server 1. One of two scenarios can occur. If there is no response from the server, the request is passed to the next RADIUS server with the next lowest index (RADIUS server 2) and so on, until the last RADIUS server is attempted (RADIUS server 5). If server 5 does not respond, the request is passed to the TACACS+ server 1. If there is no response from that server, the request is passed to the next TACACS+ server with the next lowest index (TACACS+ server 2) and so on.

If a request is sent to an active RADIUS server and the user name and password is not recognized, access is denied and passed on to the next authentication option, in this case, the TACACS+ server. The process continues until the request is either accepted, denied, or each server is queried. Finally, if the request is denied by the active TACACS+ server, the local parameters are checked for user name and password verification. This is the last chance for the access request to be accepted.



OSRG009

Figure 2: Security Flow

Vendor-Specific Attributes (VSAs)

The OS supports the configuration of Alcatel-Lucent-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are discussed in RFC 2138. VSAs must be configured when RADIUS authorization is enabled. It is up to the vendor to specify the format of their VSA. The attribute-specific field is dependent on the vendor's definition of that attribute. The Alcatel-Lucent-defined attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID field set to 6527, the vendor ID number.

Note that the PE-record entry is required in order to support the RADIUS Discovery for Layer 2 VPN feature. Note that a PE-record is only relevant if the RADIUS Discovery feature is used, not for the standard RADIUS setup.

The following RADIUS vendor-specific attributes (VSAs) are supported by Alcatel-Lucent.

- `timetra-access <ftp> <console> <both>` — This is a mandatory command that must be configured. This command specifies if the user has FTP and /or console (serial port, Telnet, and SSH) access.
- `timetra-profile <profile-name>` — When configuring this VSA for a user, it is assumed that the user profiles are configured on the local router and the following applies for local and remote authentication:
 1. The `authentication-order` parameters configured on the router must include the `local` keyword.
 2. The user name may or may not be configured on the router.
 3. The user must be authenticated by the RADIUS server
 4. Up to 8 valid profiles can exist on the router for a user. The sequence in which the profiles are specified is relevant. The most explicit matching criteria must be ordered first. The process stops when the first complete match is found.

If all the above mentioned conditions are not met, then access to the router is denied and a failed login event/trap is written to the security log.

- `timetra-default-action <permit-all|deny-all|none>` — This is a mandatory command that must be configured even if the `timetra-cmd` VSA is not used. This command specifies the default action when the user has entered a command and no entry configured in the `timetra-cmd` VSA for the user resulted in a match condition.
- `timetra-cmd <match-string>` — Configures a command or command subtree as the scope for the match condition.

The command and all subordinate commands in subordinate command levels are specified.

software supports the configuration of Alcatel-Lucent-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are discussed in RFC 2138. VSAs must be configured when RADIUS authorization is enabled. It is up to the vendor to specify the format of their VSA. The attribute-specific field is dependent on the vendor's definition of that attribute. The Alcatel-Lucent-defined attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID field set to 6527, the vendor ID number.

Note that the PE-record entry is required in order to support the RADIUS Discovery for Layer 2 VPN feature. Note that a PE-record is only relevant if the RADIUS Discovery feature is used, not for the standard RADIUS setup.

The following RADIUS vendor-specific attributes (VSAs) are supported by Alcatel-Lucent.

- `timetra-access <ftp> <console> <both>` — This is a mandatory command that must be configured. This command specifies if the user has FTP and /or console (serial port, Telnet, and SSH) access.
- `timetra-profile <profile-name>` — When configuring this VSA for a user, it is assumed that the user profiles are configured on the local router and the following applies for local and remote authentication:
 1. The authentication-order parameters configured on the router must include the local key-word.
 2. The user name may or may not be configured on the router.
 3. The user must be authenticated by the RADIUS server
 4. Up to 8 valid profiles can exist on the router for a user. The sequence in which the profiles are specified is relevant. The most explicit matching criteria must be ordered first. The process stops when the first complete match is found.

If all the above mentioned conditions are not met, then access to the router is denied and a failed login event/trap is written to the security log.

- `timetra-default-action <permit-all|deny-all|none>` — This is a mandatory command that must be configured even if the `timetra-cmd` VSA is not used. This command specifies the default action when the user has entered a command and no entry configured in the `timetra-cmd` VSA for the user resulted in a match condition.
- `timetra-cmd <match-string>` — Configures a command or command subtree as the scope for the match condition.

The command and all subordinate commands in subordinate command levels are specified.

Configure from most specific to least specific. The OS implementation exits on the first match, subordinate levels cannot be modified with subsequent action commands. Subordinate level VSAs must be entered prior to this entry to be effective.

All commands at and below the hierarchy level of the matched command are subject to the `timetra-action` VSA.

Vendor-Specific Attributes (VSAs)

Multiple match-strings can be entered in a single timetra-cmd VSA. Match strings must be semicolon (;) separated (maximum string length is 254 characters).

One or more timetra-cmd VSAs can be entered followed by a single timetra-action VSA.

- `timetra-action <deny|permit>` — Causes the permit or deny action to be applied to all match strings specified since the last timetra-action VSA.
- `timetra-home-directory <home-directory string>` — Specifies the home directory that applies for the FTP and CLI user. If this VSA is not configured, the home directory is Compact Flash slot 1 (cf1:).
- `timetra-restrict-to-home-directory <true|false>` — Specifies if user access is limited to their home directory (and directories and files subordinate to their home directory). If this VSA is not configured the user is allowed to access the entire file system.
- `timetra-login-exec <login-exec-string>` — Specifies the login exec file that is executed when the user login is successful. If this VSA is not configured no login exec file is applied.

If no VSAs are configured for a user, then the following applies:

1. The password authentication-order command on the router must include local.
2. The user name must be configured on the router.
3. The user must be successfully be authenticated by the RADIUS server
4. A valid profile must exist on the router for this user.

If all conditions listed above are not met, then access to the router is denied and a failed login event/trap is written to the security log.

The complete list of TiMetra VSAs is available on a file included on the compact flash shipped with the image.

Sample User (VSA) Configuration

The following example displays a user-specific VSA configuration. This configuration shows attributes for users named **ruser1** and **ruser2**.

The following example shows that user **ruser1** is granted console access. **ruser1**'s home directory is in compact flash slot 3 and is limited to the home directory. The default action permits all packets when matching conditions are not met. The **timetra-cmd** parameters allow or deny the user to use the **tools;telnet;configure system security** commands. Matching strings specified in the **timetra-action** command are denied for this user since the **timetra-action** is deny.

The user **ruser2** is granted FTP access. The default action denies all packets when matching conditions are not met. The **timetra-cmd** parameters allow the user to use the **configure, show,** and **debug** commands. Matching strings specified in the **timetra-action** command are permitted for this user.

```
users.timetra

ruser1  Auth-Type := System, Password == "ruser1"
        Service-Type = Login-User,
        Idle-Timeout = 600,
        Timetra-Access = console,
        Timetra-Home-Directory = cf1:
        Timetra-Restrict-To-Home = true
        Timetra-Default-Action = permit-all,
        Timetra-Cmd = "tools;telnet;configure system security",
        Timetra-Action = deny

ruser2  Auth-Type := System, Password == "ruser2"
        Service-Type = Login-User,
        Idle-Timeout = 600,
        Timetra-Access = ftp
        Timetra-Default-Action = deny-all,
        Timetra-Cmd = "configure",
        Timetra-Cmd = "show",
        Timetra-Action = permit,
        Timetra-Cmd = "debug",
        Timetra-Action = permit,
```

Vendor-Specific Attributes (VSAs)

Alcatel-Lucent Dictionary

```
# Revision: 1.29.6.2

VENDOR          Alcatel-IPD          6527

# User management VSAs
ATTRIBUTE Timetra-Access          1          integer Alcatel-IPD

VALUE          Timetra-Access          ftp          1
VALUE          Timetra-Access          console      2
VALUE          Timetra-Access          both        3

ATTRIBUTE Timetra-Home-Directory    2          string   Alcatel-IPD
ATTRIBUTE Timetra-Restrict-To-Home   3          integer  Alcatel-IPD

VALUE          Timetra-Restrict-To-Home true         1
VALUE          Timetra-Restrict-To-Home false        2

ATTRIBUTE Timetra-Profile            4          string   Alcatel-IPD
ATTRIBUTE Timetra-Default-Action     5          integer  Alcatel-IPD

VALUE          Timetra-Default-Action permit-all  1
VALUE          Timetra-Default-Action deny-all   2
VALUE          Timetra-Default-Action none        3

ATTRIBUTE Timetra-Cmd                6          string   Alcatel-IPD
ATTRIBUTE Timetra-Action              7          integer  Alcatel-IPD

VALUE          Timetra-Action          permit      1
VALUE          Timetra-Action          deny        2

ATTRIBUTE Timetra-Exec-File          8          string   Alcatel-IPD

# RADIUS subscriber authorization and CoA VSAs
ATTRIBUTE Alc-Primary-Dns            9          ipaddr   Alcatel-IPD
ATTRIBUTE Alc-Secondary-Dns          10         ipaddr   Alcatel-IPD
ATTRIBUTE Alc-Subsc-ID-Str           11         string   Alcatel-IPD
ATTRIBUTE Alc-Subsc-Prof-Str         12         string   Alcatel-IPD
ATTRIBUTE Alc-SLA-Prof-Str           13         string   Alcatel-IPD
ATTRIBUTE Alc-Force-Renew            14         string   Alcatel-IPD      # CoA
ATTRIBUTE Alc-Create-Host            15         string   Alcatel-IPD      # CoA
ATTRIBUTE Alc-ANCP-Str               16         string   Alcatel-IPD
ATTRIBUTE Alc-Retail-Serv-Id         17         integer  Alcatel-IPD
ATTRIBUTE Alc-Default-Router         18         ipaddr   Alcatel-IPD

# RADIUS subscriber accounting VSAs
ATTRIBUTE Alc-Acct-I-Inprof-Octets-64 19         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-I-Outprof-Octets-64 20         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Octets-64 21         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Octets-64 22         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-I-Inprof-Pkts-64   23         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-I-Outprof-Pkts-64  24         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Pkts-64   25         octets   Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Pkts-64  26         octets   Alcatel-IPD

ATTRIBUTE Alc-Client-Hardware-Addr    27         string   Alcatel-IPD
```

```

ATTRIBUTE Alc-Int-Dest-Id-Str          28      string  Alcatel-IPD
ATTRIBUTE Alc-Primary-Nbns            29      ipaddr  Alcatel-IPD
ATTRIBUTE Alc-Secondary-Nbns          30      ipaddr  Alcatel-IPD
ATTRIBUTE Alc-MSAP-Serv-Id            31      integer Alcatel-IPD
ATTRIBUTE Alc-MSAP-Policy              32      string  Alcatel-IPD
ATTRIBUTE Alc-MSAP-Interface          33      string  Alcatel-IPD
ATTRIBUTE Alc-PPPoE-PADO-Delay        34      integer Alcatel-IPD
ATTRIBUTE Alc-PPPoE-Service-Name      35      string  Alcatel-IPD
ATTRIBUTE Alc-DHCP-Vendor-Class-Id    36      string  Alcatel-IPD

# RADIUS subscriber accounting VSAs (HSMDA override counters)
ATTRIBUTE Alc-Acct-OC-I-Inprof-Octets-64 37      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Outprof-Octets-64 38      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Inprof-Octets-64 39      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Outprof-Octets-64 40      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Inprof-Pkts-64  41      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Outprof-Pkts-64  42      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Inprof-Pkts-64  43      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Outprof-Pkts-64  44      octets  Alcatel-IPD

ATTRIBUTE Alc-App-Prof-Str            45      string  Alcatel-IPD
ATTRIBUTE Alc-Tunnel-Group            46      string  Alcatel-IPD
ATTRIBUTE Alc-Tunnel-Algorithm        47      integer Alcatel-IPD

VALUE      Alc-Tunnel-Algorithm        weighted-access 1
VALUE      Alc-Tunnel-Algorithm        existing-first  2

ATTRIBUTE Alc-BGP-Policy              55      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Auth-Keychain       56      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Auth-Key            57      octets  Alcatel-IPD
ATTRIBUTE Alc-BGP-Export-Policy       58      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Import-Policy       59      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-PeerAS              60      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-Serv-Id           61      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-Interface         62      string  Alcatel-IPD
ATTRIBUTE Alc-IPsec-Tunnel-Template-Id 63      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-SA-Lifetime       64      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-SA-PFS-Group      65      integer Alcatel-IPD

# Match TC TmnxIkePolicyDHGroup in TIMETRA-IPSEC-MIB
VALUE      Alc-IPsec-SA-PFS-Group      group1         1
VALUE      Alc-IPsec-SA-PFS-Group      group2         2
VALUE      Alc-IPsec-SA-PFS-Group      group5         5

ATTRIBUTE Alc-IPsec-SA-Encr-Algorithm  66      integer Alcatel-IPD

# Match TC TmnxEncrAlgorithm in TIMETRA-IPSEC-MIB
VALUE      Alc-IPsec-SA-Encr-Algorithm  null           1
VALUE      Alc-IPsec-SA-Encr-Algorithm  des            2
VALUE      Alc-IPsec-SA-Encr-Algorithm  des3           3
VALUE      Alc-IPsec-SA-Encr-Algorithm  aes128         4
VALUE      Alc-IPsec-SA-Encr-Algorithm  aes192         5
VALUE      Alc-IPsec-SA-Encr-Algorithm  aes256         6

ATTRIBUTE Alc-IPsec-SA-Auth-Algorithm  67      integer Alcatel-IPD

# Match TC TmnxAuthAlgorithm in TIMETRA-IPSEC-MIB
VALUE      Alc-IPsec-SA-Auth-Algorithm  null           1
VALUE      Alc-IPsec-SA-Auth-Algorithm  md5            2

```

Vendor-Specific Attributes (VSAs)

```

VALUE      Alc-IPsec-SA-Auth-Algorithm      sha1      3

ATTRIBUTE  Alc-IPsec-SA-Replay-Window      68      integer  Alcatel-IPD

# RADIUS subscriber accounting VSAs (custom records)
ATTRIBUTE  Alc-Acct-I-High-Octets-Drop_64  69      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Low-Octets-Drop_64   70      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-High-Pack-Drop_64    71      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Low-Pack-Drop_64     72      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-High-Octets-Offer_64 73      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Low-Octets-Offer_64  74      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-High-Pack-Offer_64   75      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Low-Pack-Offer_64    76      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Unc-Octets-Offer_64  77      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-Unc-Pack-Offer_64    78      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-All-Octets-Offer_64  79      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-I-All-Pack-Offer_64    80      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-O-Inprof-Pack-Drop_64  81      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-O-Outprof-Pack-Drop_64 82      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-O-Inprof-Octs-Drop_64  83      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-O-Outprof-Octs-Drop_64 84      octets   Alcatel-IPD

# RADIUS subscriber accounting VSAs (custom records, HSMDA)
ATTRIBUTE  Alc-Acct-OC-I-All-Octs-Offer_64 85      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-I-All-Pack-Offer_64 86      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-I-Inpr-Octs-Drop_64 87      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-I-Outpr-Octs-Drop_64 88      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-I-Inpr-Pack-Drop_64 89      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-I-Outpr-Pack-Drop_64 90      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-O-Inpr-Pack-Drop_64 91      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-O-Outpr-Pack-Drop_64 92      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-O-Inpr-Octs-Drop_64 93      octets   Alcatel-IPD
ATTRIBUTE  Alc-Acct-OC-O-Outpr-Octs-Drop_64 94      octets   Alcatel-IPD

#credit control VSAs
ATTRIBUTE  Alc-Credit-Control-CategoryMap  95      string   Alcatel-IPD
ATTRIBUTE  Alc-Credit-Control-Quota        96      string   Alcatel-IPD

ATTRIBUTE  Alc-Force-Nak                    98      string   Alcatel-IPD      # CoA

```

Other Security Features

Secure Shell (SSH)

Secure Shell Version 1 (SSH) is a protocol that provides a secure, encrypted Telnet-like connection to a router. A connection is always initiated by the client (the user). Authentication takes place by one of the configured authentication methods (local, RADIUS, or TACACS+). With authentication and encryption, SSH allows for a secure connection over an insecure network.

7210 SAS-Series allows you to configure Secure Shell (SSH) Version 2 (SSH2). SSH1 and SSH2 are different protocols and encrypt at different parts of the packets. SSH1 uses server as well as host keys to authenticate systems whereas SSH2 only uses host keys. SSH2 does not use the same networking implementation that SSH1 does and is considered a more secure, efficient, and portable version of SSH.

SSH runs on top of a transport layer (like TCP or IP), and provides authentication and encryption capabilities. SSH supports remote login to another computer over a network, remote command execution, and file relocation from one host to another.

7210 SAS-Series has a global SSH server process to support inbound SSH and SCP sessions initiated by external SSH or SCP client applications. The SSH server supports SSHv1. Note that this server process is separate from the SSH and SCP client commands on the routers which initiate outbound SSH and SCP sessions.

Inbound SSH sessions are counted as inbound telnet sessions for the purposes of the maximum number of inbound sessions specified by Login Control. Inbound SCP sessions are counted as inbound ftp sessions by Login Control.

When SSH server is enabled, an SSH security key is generated. The key is only valid until either the node is restarted or the SSH server is stopped and restarted (unless the preserve-key option is configured for SSH). The key size is non-configurable and set at 1024 bits. When the server is enabled, both inbound SSH and SCP sessions will be accepted provided the session is properly authenticated.

When the global SSH server process is disabled, no inbound SSH or SCP sessions will be accepted.

When using SCP to copy files from an external device to the file system, the SCP server will accept either forward slash (“/”) or backslash (“\”) characters to delimit directory and/or filenames. Similarly, the 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 which does not get transmitted to the SCP server. For example, a destination directory specified as

Other Security Features

“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.

Exponential Login Backoff

A malicious user may attempt to gain CLI access by means of a dictionary attack using a script to automatically attempt to login as an “admin” user and using a dictionary list to test all possible passwords. Using the exponential-backoff feature in the **config>system>login-control** context the 7210 SAS increases the delay between login attempts exponentially to mitigate attacks.

A malicious user may attempt to gain CLI access by means of a dictionary attack using a script to automatically attempt to login as an “admin” user and using a dictionary list to test all possible passwords. Using the exponential-backoff feature in the **config>system>login-control** context the 7210 SAS increases the delay between login attempts exponentially to mitigate attacks.

When a user tries to login to a router using a Telnet or an SSH session, there are a limited number of attempts allowed to enter the correct password. The interval between the unsuccessful attempts change after each try (1, 2 and 4 seconds). If the system is configured for user lockout, then the user will be locked out when the number of attempts is exceeded.

However, if lockout is not configured, there are three password entry attempts allowed after the first failure, at fixed 1, 2 and 4 second intervals, in the first session, and then the session terminates. Users do not have an unlimited number of login attempts per session. After each failed password attempt, the wait period becomes longer until the maximum number of attempts is reached.

The 7210 SAS OS terminates after four unsuccessful tries. A wait period will never be longer than 4 seconds. The periods are fixed and will restart in subsequent sessions.

Note that the **config>system>login-control>[no] exponential-backoff** command works in conjunction with the **config>system>security>password>attempts** command which is also a system wide configuration.

For example:

```
*A:ALA-48>config>system# security password attempts
- attempts <count> [time <minutes1>] [lockout <minutes2>]
- no attempts

<count>           : [1..64]
<minutes1>        : [0..60]
<minutes2>        : [0..1440]
```

Exponential backoff applies to any user and by any login method such as console, SSH and Telnet.

Refer to [Configuring Login Controls on page 72](#). The commands are described in [Login, Telnet, SSH and FTP Commands on page 87](#).

User Lockout

When a user exceeds the maximum number of attempts allowed (the default is 3 attempts) during a certain period of time (the default is 5 minutes) the account used during those attempts will be locked out for a pre-configured lock-out period (the default is 10 minutes).

An security event log will be generated as soon as a user account has exceeded the number of allowed attempts and the **show>system>security>user** command can be used to display the total number of failed attempts per user.

The account will be automatically re-enabled as soon as the lock-out period has expired.

Encryption

Data Encryption Standard (DES) and Triple DES (3DES) are supported for encryption.

- DES is a widely-used method of data encryption using a private (secret) key. Both the sender and the receiver must know and use the same private key.
 - 3DES is a more secure version of the DES protocol.
-

802.1x Network Access Control

The Alcatel-Lucent 7210 SAS supports network access control of client devices (PCs, STBs, etc.) on an Ethernet network using the IEEE. 802.1x standard. 802.1x is known as Extensible Authentication Protocol (EAP) over a LAN network or EAPOL.

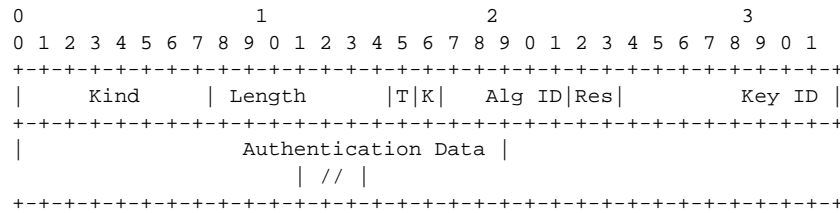
TCP Enhanced Authentication Option

The TCP Enhanced Authentication Option, currently covered in draft-bonica-tcp-auth-05.txt, Authentication for TCP-based Routing and Management Protocols, extends the previous MD5 authentication option to include the ability to change keys without tearing down the session, and allows for stronger authentication algorithms to be used.

The TCP Enhanced Authentication Option is a TCP extension that enhances security for BGP, LDP and other TCP-based protocols. This includes the ability to change keys in a BGP or LDP session seamlessly without tearing down the session. It is intended for applications where secure administrative access to both the end-points of the TCP connection is normally available.

TCP peers can use this extension to authenticate messages passed between one another. This strategy improves upon current practice, which is described in RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option. Using this new strategy, TCP peers can update authentication keys during the lifetime of a TCP connection. TCP peers can also use stronger authentication algorithms to authenticate routing messages.

Packet Formats



Option Syntax

- Kind: 8 bits
The Kind field identifies the TCP Enhanced Authentication Option. This value will be assigned by IANA.
- Length: 8 bits
The Length field specifies the length of the TCP Enhanced Authentication Option, in octets. This count includes two octets representing the Kind and Length fields.
The valid range for this field is from 4 to 40 octets, inclusive.
For all algorithms specified in this memo the value will be 16 octets.
- T-Bit: 1 bit
The T-bit specifies whether TCP Options were omitted from the TCP header for the purpose of MAC calculation. A value of 1 indicates that all TCP options other than the Extended Authentication Option were omitted. A value of 0 indicates that TCP options were included.
The default value is 0.
- K-Bit: 1 bit
This bit is reserved for future enhancement. Its value MUST be equal to zero.
- Alg ID: 6 bits
The Alg ID field identifies the MAC algorithm.
- Res: 2 bits
These bits are reserved. They MUST be set to zero.
Key ID: 6 bits
The Key ID field identifies the key that was used to generate the message digest.
- Authentication Data: Variable length
- The Authentication Data field contains data that is used to authenticate the TCP segment. This data includes, but need not be restricted to, a MAC. The length and format of the Authentication Data Field can be derived from the Alg ID.

- The Authentication for TCP-based Routing and Management Protocols draft provides an overview of the TCP Enhanced Authentication Option. The details of this feature are described in draft-bonica-tcp-auth-04.txt.

Keychain

A keychain is a set of up to 64 keys, where each key is $\{A[i], K[i], V[i], S[i], T[i], S'[i], T'[i]\}$ as described in draft-bonica-tcp-auth-05.txt, *Authentication for TCP-based Routing and Management Protocols*. The keys can be assigned to both sides of a LDP peer. The individual keys in a keychain have a begin- and end-time indicating when to use this key.

These fields map to the CLI tree as:

Table 4: Keychain Mapping

Field	Definition	CLI
i	The key identifier expressed as an integer (0...63)	config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
A[i]	Authentication algorithm to use with key[i]	config>system>security>keychain>direction>bi>entry with algorithm <i>algorithm</i> parameter. config>system>security>keychain>direction>uni>receive>entry with algorithm <i>algorithm</i> parameter. config>system>security>keychain>direction>uni>send>entry with algorithm <i>algorithm</i> parameter.
K[i]	Shared secret to use with key[i].	config>system>security>keychain>direction>uni>receive>entry with shared secret parameter config>system>security>keychain>direction>uni>send>entry with shared secret parameter config>system>security>keychain>direction>bi>entry with shared secret parameter
V[i]	A vector that determines whether the key[i] is to be used to generate MACs for inbound segments, outbound segments, or both.	config>system>security>keychain>direction
S[i]	Start time from which key[i] can be used by sending TCPs.	config>system>security>keychain>direction>bi>entry>begin-time config>system>security>keychain>direction>uni>send>entry >begin-time
T[i]	End time after which key[i] cannot be used by sending TCPs.	Inferred by the begin-time of the next key (youngest key rule).
S'[i]	Start time from which key[i] can be used by receiving TCPs.	config>system>security>keychain>direction>bi>entry>begin-time config>system>security>keychain>direction>bi>entry>tolerance config>system>security>keychain>direction>uni>receive>entry >begin-time config>system>security>keychain>direction>uni>receive>entry >tolerance
T'[i]	End time after which key[i] cannot be used by receiving TCPs	config>system>security>keychain>direction>uni>receive>entry>end-time

Configuration Notes

This section describes security configuration caveats.

General

- If a RADIUS or a TACACS+ server is not configured, then password, profiles, and user access information must be configured on each router in the domain.
- If a RADIUS authorization is enabled, then VSAs must be configured on the RADIUS server

Configuring Security with CLI

This section provides information to configure security using the command line interface.

Topics in this section include:

- [Setting Up Security Attributes on page 48](#)
 - [Configuring Authorization on page 49](#)
 - [Configuring Authorization on page 49](#)
 - [Configuring Accounting on page 51](#)
- [Configuration Tasks on page 54](#)
- [Security Configuration Procedures on page 55](#)
 - [Configuring Management Access Filters on page 55](#)
 - [Configuring Password Management Parameters on page 56](#)
 - [Configuring Profiles on page 57](#)
 - [Configuring Users on page 58](#)
 - [Copying and Overwriting Users and Profiles on page 60](#)
 - [Enabling SSH on page 71](#)
 - [Configuring Login Controls on page 72](#)
 - [RADIUS Configurations on page 64](#)
 - [Configuring RADIUS Authentication on page 64](#)
 - [Configuring RADIUS Authorization on page 65](#)
 - [Configuring RADIUS Accounting on page 66](#)
 - [TACACS+ Configurations on page 67](#)
 - [Enabling TACACS+ Authentication on page 67](#)
 - [Configuring TACACS+ Authorization on page 69](#)
 - [Configuring TACACS+ Accounting on page 70](#)

Setting Up Security Attributes

Configuring Authentication

Refer to the following sections to configure authentication:

- Local authentication
 - [Configuring Password Management Parameters on page 56](#)
 - [Configuring Profiles on page 57](#)
 - [Configuring Users on page 58](#)
- RADIUS authentication (only)

By default, authentication is enabled locally. Perform the following tasks to configure security on each participating router:

 - [Configuring Profiles on page 57](#)
 - [Configuring RADIUS Authentication on page 64](#)
 - [Configuring Users on page 58](#)
- RADIUS authentication
To implement only RADIUS authentication, *with* authorization, perform the following tasks on each participating router:
 - [Configuring RADIUS Authentication on page 64](#)
 - [Configuring RADIUS Authorization on page 65](#)
- TACACS+ authentication
To implement only TACACS+ authentication, perform the following tasks on each participating router:
 - [Configuring Profiles on page 57](#)
 - [Configuring Users on page 58](#)
 - [Enabling TACACS+ Authentication on page 67](#)

Configuring Authorization

Refer to the following sections to configure authorization.

- Local authorization
For local authorization, configure these tasks on each participating router:
 - [Configuring Profiles on page 57](#)
 - [Configuring Users on page 58](#)

- RADIUS authorization (only)
For RADIUS authorization (without authentication), configure these tasks on each participating router:
 - [Configuring RADIUS Authorization on page 65](#)
 - [Configuring Profiles on page 57](#)For RADIUS authorization, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 30](#).

- RADIUS authorization
For RADIUS authorization (with authentication), configure these tasks on each participating router:
 - [Configuring RADIUS Authorization on page 65](#)
For RADIUS authorization, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 30](#).
 - [Configuring RADIUS Authentication on page 64](#)
 - [Configuring Profiles on page 57](#)

- TACACS+ authorization (only)
For TACACS+ authorization (without authentication), configure these tasks on each participating router:
 - [Configuring TACACS+ Authorization on page 69](#)

- TACACS+ authorization

Setting Up Security Attributes

For TACACS+ authorization (with authentication), configure these tasks on each participating router:

- [Enabling TACACS+ Authentication on page 67](#)
- [Configuring TACACS+ Authorization on page 69](#)

Configuring Accounting

Refer to the following sections to configure accounting.

- Local accounting is not implemented. For information about configuring accounting policies, refer to [Configuring Logging with CLI on page 271](#)
- [Configuring RADIUS Accounting on page 66](#)
- [Configuring TACACS+ Accounting on page 70](#)

Security Configurations

This section provides information to configure security and configuration examples of configuration tasks.

To implement security features, configure the following components:

- Management access filters
- Profiles
- User access parameters
- Password management parameters
- Enable RADIUS and/or TACACS+
 - One to five RADIUS and/or TACACS+ servers
 - RADIUS and/or TACACS+ parameters

The following example displays default values for security parameters.

```
A:ALA-1>config>system>security# info detail
-----
no hash-control
telnet-server
no telnet6-server
no ftp-server
management-access-filter
exit
profile "default"
  default-action none
  no li
  entry 10
    no description
    match "exec"
    action permit
...
password
  authentication-order radius tacplus local
  no aging
  minimum-length 6
  attempts 3 time 5 lockout 10
  complexity
exit
user "admin"
  password "./3kQWERTYn0Q6w" hash
  access console
no home-directory
no restricted-to-home
  console
    no login-exec
    no cannot-change-password
    no new-password-at-login
  member "administrative"
exit
```

```
exit
snmp
    view iso subtree 1
        mask ff type included
    exit
...
    access group snmp-ro security-model snmpv1 security-level no-auth-no-privacy read
no-security notify no-security
    access group snmp-ro security-model snmpv2c security-level no-auth-no-privacy
read no-security notify no-security
    access group snmp-rw security-model snmpv1 security-level no-auth-no-privacy read
no-security write no-security notify no-security
    access group snmp-rw security-model snmpv2c security-level no-auth-no-privacy
read no-security write no-security notify no-security
    access group snmp-rwa security-model snmpv1 security-level no-auth-no-privacy
read iso write iso notify iso
    access group snmp-rwa security-model snmpv2c security-level no-auth-no-privacy
read iso write iso notify iso
    access group snmp-trap security-model snmpv1 security-level no-auth-no-privacy
notify iso
    access group snmp-trap security-model snmpv2c security-level no-auth-no-privacy
notify iso
    access group cli-readonly security-model snmpv2c security-level
no-auth-no-privacy read iso notify iso
    access group cli-readwrite security-model snmpv2c security-level
no-auth-no-privacy read iso write iso notify iso
    attempts 20 time 5 lockout 10
exit
no ssh
```

Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure security and provides the CLI commands. [Table 5](#) depicts the capabilities of authentication, authorization, and accounting configurations. For example, authentication can be enabled locally and on RADIUS and TACACS+ servers. Authorization can be executed locally, on a RADIUS server, or on a TACACS+ server. Accounting can be performed on a RADIUS or TACACS+ server.

Table 5: Security Configuration Requirements

Authentication	Authorization	Accounting
Local	Local	None
RADIUS	Local and RADIUS	RADIUS
TACACS+	Local	TACACS+

Security Configuration Procedures

- [Configuring Management Access Filters on page 55](#)
- [Configuring Password Management Parameters on page 56](#)
- [Configuring Profiles on page 57](#)
- [Configuring Users on page 58](#)
- [Copying and Overwriting Users and Profiles on page 60](#)
- [Enabling SSH on page 71](#)

Configuring Management Access Filters

NOTE:

- IPv4 is supported on 7210 SAS-Sx devices. IPv6 is not supported on 7210 SAS-Sx devices.

Creating and implementing management access filters is optional. Management access filters control all traffic going in to the CPM, including all routing protocols. They apply to packets from all ports. The filters can be used to restrict management of the 7210 SAS router by other nodes outside either specific (sub)networks or through designated ports. By default, there are no filters associated with security options. The management access filter and entries must be explicitly created on each router. These filters also apply to the management Ethernet port.

The 7210 SAS implementation exits the filter when the first match is found and execute the actions according to the specified action. For this reason, entries must be sequenced correctly from most to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword CPM to be considered complete. Entries without the action keyword are considered incomplete and will be rendered inactive.

Use the following CLI commands to configure a management access filter. This example only accepts packets matching the criteria specified in entries 1 and 2. Non-matching packets are denied.

CLI Syntax:

```
config>system
  security
    management-access-filter
      ip-filter
```

```

ipv6-filter
  default-action {permit|deny|deny-host-unreachable}
  renum old-entry-number new-entry-number
  no shutdown
  entry entry-id
    description description-string
    src-port {port-id cpm|laglag-id}
    src-ip {ip-prefix/mask | ip-prefix netmask}
    protocol protocol-id
    dst-port port [mask]
    action {permit|deny|deny-host-unreachable}
    log
  
```

Configuring Password Management Parameters

Password management parameters consists of defining aging, the authentication order and authentication methods, password length and complexity, as well as the number of attempts a user can enter a password.

Depending on the your authentication requirements, password parameters are configured locally.

Use the following CLI commands to configure password support:

CLI Syntax:

```

config>system>security
  password
    admin-password password [hash|hash2]
    aging days
    attempts count [time minutes1] [lockout minutes2]
    authentication-order [method-1] [method-2] [method-3]
      [exit-on-reject]
    complexity [numeric] [special-character] [mixed-case]
    health-check
    minimum-length value
  
```

The following example displays a password configuration:

```

A:ALA-1>config>system>security# info
-----
  password
  authentication-order radius tacplus local
  aging 365
  minimum-length 8
  attempts 5 time 5 lockout 20
  exit
-----
A:ALA-1>config>system>security#
  
```

Configuring Profiles

Profiles are used to deny or permit access to a hierarchical branch or specific commands. Profiles are referenced in a user configuration. A maximum of sixteen user profiles can be defined. A user can participate in up to sixteen profiles. Depending on the the authorization requirements, passwords are configured locally or on the RADIUS server.

Use the following CLI commands to configure user profiles:

```
CLI Syntax: config>system>security
                profile user-profile-name
                  default-action {deny-all|permit-all|none}
                  renum old-entry-number new-entry-number
                  entry entry-id
                    description description-string
                    match command-string
                    action {permit|deny}
```

The following example displays a user profile output:

```
A:ALA-1>config>system>security# info
-----
...
    profile "ghost"
      default-action permit-all
      entry 1
        match "configure"
        action permit
      exit
      entry 2
        match "show"
      exit
      entry 3
        match "exit"
      exit
    exit
...
-----
A:ALA-1>config>system>security#
```

Configuring Users

Configure access parameters for individual users. For user, define the login name for the user and, optionally, information that identifies the user. Use the following CLI commands to configure RADIUS support:

```
CLI Syntax: config>system>security
               user-template template-name
               user user-name
               access [ftp] [snmp] [console]
               console
                 cannot-change-password
                 login-exec url-prefix:source-url
                 member user-profile-name [user-profile-name...(up to 8
                 max)]
                 new-password-at-login
               home-directory url-prefix [directory][directory/directory
               ..]
               password [password] [hash|hash2]
               restricted-to-home
               snmp
                 authentication {[none]}|[hash] {md5 key-1|sha key-1} pri-
                 vacy {none|des-key key-2}}
               group group-name
```

The following displays a user configuration example:

```
A:ALA-1>config>system>security# info
-----
...
      user "49ers"
        password "qQbnuzLd7H/VxGdUqdh7bE" hash2
        access console ftp snmp
        restricted-to-home
        console
          member "default"
          member "ghost"
        exit
      exit
...
-----
A:ALA-1>config>system>security#
```

Configuring Keychains

The following displays a keychain configuration.

```
A:ALA-1>config>system>security# info
-----
...
    keychain "abc"
        direction
            bi
                entry 1 key "ZcvSElJzJx/wBZ9biCtOVQJ9YZQvVU.S" hash2 alg
algorithm aes-128-cmac-96
                begin-time 2006/12/18 22:55:20
                exit
            exit
        exit
    exit
    keychain "basasd"
        direction
            uni
                receive
                    entry 1 key "Ee7xdKlYO2D0m7v3IJv/84LIu96R2fZh" hash2
algorithm aes-128-cmac-96
                    tolerance forever
                exit
            exit
        exit
    exit
    exit
...
-----
A:ALA-1>config>system>security#
```

Copying and Overwriting Users and Profiles

You can copy a profile or user. You can copy a profile or user or overwrite an existing profile or user. The **overwrite** option must be specified or an error occurs if the destination profile or username already exists.

User

CLI Syntax: `config>system>security# copy {user source-user | profile source-profile} to destination [overwrite]`

Example:

```
config>system>security# copy user testuser to testuserA
MINOR: CLI User "testuserA" already exists - use overwrite
flag.
config>system>security#
config>system>security# copy user testuser to testuserA
overwrite
config>system>security#
```

The following output displays the copied user configurations:

```
A:ALA-12>config>system>security# info
-----
...
    user "testuser"
        password "F6XjryaATzM" hash
        access snmp
        snmp
            authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
            group "testgroup"
        exit
    exit
    user "testuserA"
        password "" hash2
        access snmp
        console
            new-password-at-login
        exit
        snmp
            authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
            group "testgroup"
        exit
    exit
...
-----
A:ALA-12>config>system>security# info
```

Note that the cannot-change-password flag is not replicated when a copy user command is performed. A new-password-at-login flag is created instead.

```
A:ALA-12>config>system>security>user# info
-----
password "F6XjryaATzM" hash
access snmp
console
    cannot-change-password
exit
snmp
    authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
    group "testgroup"
exit
-----
A:ALA-12>config>system>security>user# exit
A:ALA-12>config>system>security# user testuserA
A:ALA-12>config>system>security>user# info
-----
password "" hash2
access snmp
console
    new-password-at-login
exit
snmp
    authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
    group "testgroup"
exit
-----
A:ALA-12>config>system>security>user#
```

Profile

CLI Syntax: config>system>security# copy {user source-user | profile source-profile} to destination [overwrite]

Example: config>system>security# copy profile default to testuser

The following output displays the copied profiles:

```
A:ALA-49>config>system>security# info
-----
...
A:ALA-49>config>system>security# info detail
-----
...
        profile "default"
            default-action none
            entry 10
                no description
                match "exec"
                action permit
            exit
            entry 20
                no description
                match "exit"
                action permit
            exit
            entry 30
                no description
                match "help"
                action permit
            exit
            entry 40
                no description
                match "logout"
                action permit
            exit
            entry 50
                no description
                match "password"
                action permit
            exit
            entry 60
                no description
                match "show config"
                action deny
            exit
            entry 70
                no description
                match "show"
                action permit
            exit
            entry 80
                no description
                match "enable-admin"
```

```
        action permit
    exit
exit
profile "testuser"
    default-action none
    entry 10
        no description
        match "exec"
        action permit
    exit
    entry 20
        no description
        match "exit"
        action permit
    exit
    entry 30
        no description
        match "help"
        action permit
    exit
    entry 40
        no description
        match "logout"
        action permit
    exit
    entry 50
        no description
        match "password"
        action permit
    exit
    entry 60
        no description
        match "show config"
        action deny
    exit
    entry 70
        no description
        match "show"
        action permit
    exit
    entry 80
        no description
        match "enable-admin"
        action permit
    exit
exit
profile "administrative"
    default-action permit-all exit
...
-----
A:ALA-12>config>system>security#
```

RADIUS Configurations

- [Configuring RADIUS Authentication on page 64](#)
- [Configuring RADIUS Authorization on page 65](#)
- [Configuring RADIUS Accounting on page 66](#)
- [Configuring 802.1x RADIUS Policies on page 67](#)

Configuring RADIUS Authentication

RADIUS is disabled by default and must be explicitly enabled. The mandatory commands to enable RADIUS on the local router are **radius** and `server server-index address ip-address secret key`.

Also, the system IP address must be configured in order for the RADIUS client to work. See [Configuring a System Interface of the](#) .

The other commands are optional. The `server` command adds a RADIUS server and configures the RADIUS server's IP address, index, and key values. The `index` determines the sequence in which the servers are queried for authentication requests.

On the local router, use the following CLI commands to configure RADIUS authentication:

CLI Syntax:

```
config>system>security
radius
port port
retry count
server server-index address ip-address secret key
timeout seconds
no shutdown
```

The following displays a RADIUS authentication configuration example:

```
A:ALA-1>config>system>security# info
-----
retry 5
timeout 5
server 1 address 10.10.10.103 secret "test1"
server 2 address 10.10.0.1 secret "test2"
server 3 address 10.10.0.2 secret "test3"
server 4 address 10.10.0.3 secret "test4"
...
-----
A:ALA-1>config>system>security#
```

Configuring RADIUS Authorization

In order for RADIUS authorization to function, RADIUS authentication *must* be enabled first. See [Configuring RADIUS Authentication on page 64](#).

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 30](#).

On the local router, use the following CLI commands to configure RADIUS authorization:

```
CLI Syntax: config>system>security
               radius
               authorization
```

The following displays a RADIUS authorization configuration example:

```
A:ALA-1>config>system>security# info
-----
...
    radius
        authorization
        retry 5
        timeout 5
        server 1 address 10.10.10.103 secret "test1"
        server 2 address 10.10.0.1 secret "test2"
        server 3 address 10.10.0.2 secret "test3"
        server 4 address 10.10.0.3 secret "test4"
    exit
...
-----
A:ALA-1>config>system>security#
```

Configuring RADIUS Accounting

On the local router, use the following CLI commands to configure RADIUS accounting:

```
CLI Syntax: config>system>security
               radius
               accounting
```

The following displays RADIUS accounting configuration example:

```
A:ALA-1>config>system>security# info
-----
...
    radius
    shutdown
    authorization
    accounting
    retry 5
    timeout 5
    server 1 address 10.10.10.103 secret "test1"
    server 2 address 10.10.0.1 secret "test2"
    server 3 address 10.10.0.2 secret "test3"
    server 4 address 10.10.0.3 secret "test4"
    exit
...
-----
A:ALA-1>config>system>security#
```

Configuring 802.1x RADIUS Policies

Use the following CLI commands to configure generic authentication parameters for clients using 802.1x EAPOL. Additional parameters are configured per Ethernet port. Refer to the 7210 SAS OS M, X Interface Configuration Guide.

To configure generic parameters for 802.1x authentication, enter the following CLI syntax.

```
CLI Syntax: config>system>security
                dot1x
                  radius-plcy policy-name
                    server server-index address ip-address secret key [port
                      port]
                    source-address ip-address
                    no shutdown
```

The following displays a 802.1x configuration example:

```
A:ALA-1>config>system>security# info
-----
                dot1x
                  radius-plcy "dot1x_plcy" create
                    server 1 address 1.1.1.1 port 65535 secret "a"
                    server 2 address 1.1.1.2 port 6555 secret "a"
                    source-address 1.1.1.255
                    no shutdown
                ...
-----
A:ALA-1>config>system#
```

TACACS+ Configurations

- [Enabling TACACS+ Authentication on page 67](#)
- [Configuring TACACS+ Authorization on page 69](#)
- [Configuring TACACS+ Accounting on page 70](#)

Enabling TACACS+ Authentication

To use TACACS+ authentication on the router, configure one or more TACACS+ servers on the network.

Configuring 802.1x RADIUS Policies

Use the following CLI commands to configure profiles:

```
CLI Syntax: config>system>security
               tacplus
                 server server-index address ip-address secret key
                 timeout seconds
                 no shutdown
```

The following displays a TACACS+ authentication configuration example:

```
A:ALA-1>config>system>security>tacplus# info
-----
          timeout 5
          server 1 address 10.10.0.5 secret "test1"
          server 2 address 10.10.0.6 secret "test2"
          server 3 address 10.10.0.7 secret "test3"
          server 4 address 10.10.0.8 secret "test4"
          server 5 address 10.10.0.9 secret "test5"
-----
A:ALA-1>config>system>security>tacplus#
```

Configuring TACACS+ Authorization

In order for TACACS+ authorization to function, TACACS+ authentication *must* be enabled first. See [Enabling TACACS+ Authentication on page 67](#).

On the local router, use the following CLI commands to configure RADIUS authorization:

CLI Syntax: config>system>security
tacplus
authorization
no shutdown

The following displays a TACACS+ authorization configuration example:

```
A:ALA-1>config>system>security>tacplus# info
-----
      authorization
      timeout 5
      server 1 address 10.10.0.5 secret "test1"
      server 2 address 10.10.0.6 secret "test2"
      server 3 address 10.10.0.7 secret "test3"
      server 4 address 10.10.0.8 secret "test4"
      server 5 address 10.10.0.9 secret "test5"
-----
A:ALA-1>config>system>security>tacplus#
```

Configuring TACACS+ Accounting

On the local router, use the following CLI commands to configure TACACS+ accounting:

```
CLI Syntax: config>system>security
               tacplus
               accounting
```

The following displays a TACACS+ accounting configuration example:

```
A:ALA-1>config>system>security>tacplus# info
-----
      accounting
      authorization
      timeout 5
      server 1 address 10.10.0.5 secret "test1"
      server 2 address 10.10.0.6 secret "test2"
      server 3 address 10.10.0.7 secret "test3"
      server 4 address 10.10.0.8 secret "test4"
      server 5 address 10.10.0.9 secret "test5"
-----
A:ALA-1>config>system>security>tacplus#
```

Enabling SSH

Use the SSH command to configure the SSH server as SSH1, SSH2 or both. The default is SSH2 (SSH version 2). This command should only be enabled or disabled when the SSH server is disabled. This setting should not be changed while the SSH server is running since the actual change only takes place after SSH is disabled or enabled.

CLI Syntax: `config>system>security`
`ssh`
`preserve-key`
`no server-shutdown`
`version ssh-version`

The following displays a SSH server configuration as both SSH and SSH2 using a host-key:

```
A:sim1>config>system>security>ssh# info
-----
                preserve-key
                version 1-2
-----
A:sim1>config>system>security>ssh#
```

Configuring Login Controls

Configure login control parameters for console, Telnet, and FTP sessions.

To configure login controls, enter the following CLI syntax.

```
CLI Syntax: config>system
                login-control
                  exponential-backoff
                  ftp
                    inbound-max-sessions value
                  telnet
                    inbound-max-sessions value
                    outbound-max-sessions value
                  idle-timeout {minutes |disable}
                  pre-login-message login-text-string [name]
                  login-banner
                  motd {url url-prefix: source-url|text motd-text-string}
```

The following displays a login control configuration example:

```
A:ALA-1>config>system# info
-----
...
    login-control
      ftp
        inbound-max-sessions 5
      exit
      telnet
        inbound-max-sessions 7
        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
    no exponential-backoff
...
-----
A:ALA-1>config>system#
```

Security Command Reference

Command Hierarchies

Configuration Commands

- [Security Commands](#)
 - [Password Com on page 76](#)
 - [Profile Commands on page 76](#)
 - [RADIUS Commands on page 76](#)
 - [SSH Commands on page 77](#)
 - [TACACS+ Commands on page 77](#)
 - [User Commands on page 77](#)
 - [Dot1x Commands on page 78](#)
 - [Keychain Commands on page 79](#)
 - [TCP Enhanced Authentication Commands on page 79](#)
- [Login Control Commands on page 79](#)
- [IPsec Commands on page 80](#)
- [Show Commands on page 81](#)
- [Login Control on page 81](#)
- [Clear Commands on page 81](#)
- [Debug Commands on page 81](#)

Security Commands

```
config
  — system
    — security
      — copy {user source-user | profile source-profile} to destination [overwrite]
      — dot1x
      — [no] ftp-server
      — hash-control [read-version {1 | 2 | all}] [write-version {1 | 2}]
      — no hash-control
      — [no] keychain keychain-name
      — management-access-filter
      — password
      — [no] profile user-profile-name
      — [no] radius
      — snmp
      — source-address
        — application app [ip-int-name|ip-address]
        — no application app
        — application6 app [ipv6-address]
        — no application6 app
      — [no] telnet-server
      — [no] telnet6-server
      — ssh
      — [no] tacplus
      — [no] users user-name
      — user-template {tacplus_default | radius_default}
```

Management Access Filter Commands

NOTE: IPv6 for management access filters is not supported on 7210 SAS-Sx.

```

config
  — system
    — security
      — [no] management-access-filter
        — [no] ip-filter
          — default-action {permit | deny | deny-host-unreachable}
          — [no] entry entry-id
            — action {permit | deny | deny-host-unreachable}
            — no action
            — description description-string
            — no description
            — dst-port port [mask]
            — no dst-port
            — fragment {true|false}
            — no fragment
            — l4-src-port port [mask]
            — no l4-src-port
            — [no] log
            — protocol protocol-id
            — no protocol
            — router router-instance
            — no router
            — src-ip {ip-prefix/mask | ip-prefix netmask}
            — no src-ip
            — src-port {port-id | lag lag-id }
            — no src-port
        — [no]ipv6-filter
          — default-action {permit | deny | deny-host-unreachable}
          — [no] entry entry-id
            — action {permit | deny | deny-host-unreachable}
            — no action
            — description description-string
            — no description
            — dst-port port [mask]
            — no dst-port
            — flow-label value
            — no flow-label
            — l4-src-port port [mask]
            — no l4-src-port
            — [no] log
            — next-header next-header
            — no next-header
            — router router-instance
            — no router
            — src-ip {ip-prefix/prefix-length | <ip-prefix> <netmask>}
            — no src-ip
            — src-port {port-id | lag lag-id }
            — no src-port
        — renum old-entry-number new-entry-number
        — [no] shutdown

```

Security Password Commands

```

config
  — system
    — security
      — password
        — admin-password password [hash | hash2]
        — no admin-password
        — aging days
        — no aging
        — attempts count [time minutes1] [lockout minutes2]
        — no attempts
        — authentication-order [method-1] [method-2] [method-3] [exit-on-reject]
        — no authentication-order
        — [no] complexity [numeric] [special-character] [mixed-case]
        — [no] health-check [interval interval]
        — minimum-length value
        — no minimum-length
  
```

Profile Commands

```

config
  — system
    — security
      — [no] profile user-profile-name
        — default-action {deny-all | permit-all | none}
        — [no] entry entry-id
          — action {deny | permit}
          — description description-string
          — no description
          — match command-string
          — no match
        — renum old-entry-number new-entry-number
  
```

RADIUS Commands

```

config
  — system
    — security
      — [no] radius
        — [no] accounting
        — accounting-port port
        — no accounting-port
        — [no] authorization
        — port port
        — no port
        — retry count
        — no retry
        — server server-index address ip-address secret key [hash | hash2]
        — no server server-index
        — [no] shutdown
        — timeout seconds
        — no timeout
        — [no] use-default-template
  
```

SSH Commands

```

config
  — system
    — security
      — ssh
        — [no] preserve-key
        — [no] server-shutdown
        — [no] version SSH-version

```

TACPLUS Commands

```

config
  — system
    — security
      — [no] tacplus
        — accounting [record-type {start-stop | stop-only}]
        — no accounting
        — [no] authorization
        — server server-index address ip-address secret key [hash | hash2] [port port]
        — no server server-index
        — [no] shutdown
        — timeout seconds
        — no timeout
        — [no] use-default-template

```

User Commands

```

config
  — system
    — security
      — [no] users user-name
        — [no] access [ftp] [snmp] [console]
        — console
          — [no] cannot-change-password
          — login-exec url-prefix::source-url
          — no login-exec
          — member user-profile-name [user-profile-name...(up to 8 max)]
          — no member user-profile-name
          — [no] new-password-at-login
        — home-directory url-prefix [directory] [directory/directory...]
        — no home-directory
        — password [password] [hash | hash2]
        — [no] restricted-to-home
        — snmp
          — authentication {[none] | [[hash] {md5 key-1 | sha key-1 } privacy {privacy-level key-2}]
          — group group-name
          — no group

```

User Template Commands

```

config
  — system
    — security

```

- **user-template** {tacplus_default | radius_default}
 - [no] **access** [ftp] [console]
 - **console**
 - **login-exec** *url-prefix:source-url*
 - **no login-exec**
 - **home-directory** *url-prefix [directory][directory/directory..]*
 - **no home-directory**
 - [no] **restricted-to-home**

Dot1x Commands

- config
 - system
 - **security**
 - **dot1x**
 - **radius-plcy** *name [create]*
 - **retry** *count*
 - **no retry**
 - **server** *server-index address ip-address secret key [hash|hash2]*
[**auth-port** *auth-port*] [**acct-port** *acct-port*] [**type** *server-type*]
 - **source-address** *ip-address*
 - [no] **shutdown**
 - **timeout** *seconds*
 - **no timeout**
 - [no] **shutdown**

Keychain Commands

```

config
  — system
    — security
      — [no] keychain keychain-name
        — description description-string
        — no description
        — direction {uni | bi}
          — bi
            — entry {null-key | entry-id key authentication-key | hash-key | hash2-key [hash | hash2] algorithm algorithm}
            — no entry {null-key | entry-id}
            — begin-time [date] [hours-minutes] [UTC] {now | forever}
            — [no] shutdown
            — tolerance [seconds | forever]
          — uni
            — receive
              — entry {null-key | entry-id key authentication-key | hash-key | hash2-key [hash | hash2] algorithm algorithm}
              — no entry {null-key | entry-id}
              — begin-time [date] [hours-minutes] [UTC] {now | forever}
              — end-time [date][hours-minutes] [UTC] {now | forever}
              — [no] shutdown
              — tolerance [seconds | forever]
            — send
              — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
              — begin-time [date] [hours-minutes] [UTC] {now | forever}
              — [no] shutdown
          — [no] shutdown
        — tcp-option-number
          — receive option-number
          — send option-number

```

Login Control Commands

```

config
  — system
    — login-control
      — [no] exponential-backoff
      — ftp
        — inbound-max-sessions value
        — no inbound-max-sessions
      — idle-timeout {minutes | disable}
      — no idle-timeout
      — [no] login-banner
      — motd {url url-prefix: source-url | text motd-text-string}
      — no motd
      — pre-login-message login-text-string [name]

```

- **no pre-login-message**
- **ssh**
 - **disable-graceful-shutdown**
 - **inbound-max-sessions**
 - **outbound-max-sessions**
- **telnet**
 - **enable-graceful-shutdown**
 - **inbound-max-sessions** *value*
 - **no inbound-max-sessions**
 - **outbound-max-sessions** *value*
 - **no outbound-max-sessions**

IPsec Commands

- config**
 - **ipsec**
 - **[no] static-sa** *sa-name*
 - **authentication** *md5 / sha1 {ascii-key ascii-key / hex-key hex-key}*
 - **no authentication**
 - **description** *description-string*
 - **no description**
 - **direction** *inbound / outbound / bidirectional*
 - **no direction**
 - **protocol** *ah / esp*
 - **no protocol**
 - **spi** *spi-key*

Show Commands

Security

```

show
  — system
    — security
      — access-group [group-name]
      — authentication [statistics]
      — communities
      — keychain [key-chain] [detail]
      — management-access-filter
        — ip-filter [entry entry-id]
        — ipv6-filter [entry entry-id]
      — password-options
      — profile [user-profile-name]
      — source-address
      — ssh
      — user [user-id] [detail]
      — view [view-name] [detail]

show
  — ipsec
    — static-sa
    — static-sa name sa-name
    — static-sa spi spi

```

Login Control

```

show
  — users

```

Clear Commands

```

admin
  — user user-name
    — clear-lockout

```

Debug Commands

```

debug
  — radius [detail] [hex]
  — no radius

```

Configuration Commands

General Security Commands

description

Syntax	description <i>description-string</i> no description
Context	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry config>sys>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
Description	This command creates a text description stored in the configuration file for a configuration context. This command associates a text string with a configuration context to help identify the context in the configuration file. The no form of the command removes the string.
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.

shutdown

Syntax	[no] shutdown
Context	config>system>security>mgmt-access-filter config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
Description	The shutdown command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. 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 the command puts an entity into the administratively enabled state.
Default	no shutdown

security

Syntax	security
Context	config>system
Description	<p>This command creates the context to configure security settings.</p> <p>Security commands manage user profiles and user membership. Security commands also manage user login registrations.</p>

ftp-server

Syntax	[no] ftp-server
Context	config>system>security
Description	<p>This command enables FTP servers running on the system.</p> <p>FTP servers are disabled by default. At system startup, only SSH server are enabled.</p> <p>The no form of the command disables FTP servers running on the system.</p>

hash-control

Syntax	hash-control [read-version {1 2 all}] [write-version {1 2}] no hash-control
Context	config>system>security
Description	<p>Whenever the user executes a save or info command, the system will encrypt all passwords, MD5 keys, etc., for security reasons. At present, two algorithms exist.</p> <p>The first algorithm is a simple, short key that can be copied and pasted in a different location when the user wants to configure the same password. However, because it is the same password and the hash key is limited to the password/key, even the casual observer will notice that it is the same key.</p> <p>The second algorithm is a more complex key, and cannot be copied and pasted in different locations in the configuration file. In this case, if the same key or password is used repeatedly in different contexts, each encrypted (hashed) version will be different.</p>
Default	all — read-version set to accept both versions 1 and 2
Parameters	<p>read-version {1 2 all} — When the read-version is configured as “all,” both versions 1 and 2 will be accepted by the system. Otherwise, only the selected version will be accepted when reading configuration or exec files. The presence of incorrect hash versions will abort the script/startup.</p> <p>write-version {1 2} — Select the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.</p>

source-address

Syntax	source-address
Context	config>system>security
Description	<p>This command specifies the source address that should be used in all unsolicited packets sent by the application.</p> <p>This feature only applies on in-band interfaces and does not apply on the out-band management interface. Packets going out the management interface will keep using that as source IP address. IN other words, when the RADIUS server is reachable through both the management interface and a network interface, the management interface is used despite whatever is configured under the source-address statement.</p>

application

Syntax	application <i>app</i> [<i>ip-int-name</i> <i>ip-address</i>] no application <i>app</i>
Context	config>system>security>source-address
Description	This command specifies the application to use the source-IP address specified by the source-address command.
Parameters	<p><i>app</i> — Specify the application name.</p> <p>Values telnet, ftp, ssh, radius, tacplus, snmptrap, syslog, ping, traceroute, dns, sntp, ntp, ptp NOTE: PTP is not supported on all platforms. Only the applications supported on the platform can be used as a value with this command. Using an unsupported application value will not have the desired effect.</p> <p><i>ip-int-name</i> / <i>ip-address</i> — Specifies the name of the IP interface, IP address . If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p>

application6

Syntax	application6 <i>app</i> [<i>ipv6-address</i>] no application6 <i>app</i>
Context	config>system>security>source-address
Description	This command specifies the application to use the source IPv6 address specified by the source address.
Parameters	<p><i>app</i> — Specify the application name.</p> <p>Values dns ftp ping radius snmptrap syslog tacplus telnet traceroute</p> <p><i>ipv6-address</i> — Specifies the name of the IPv6 address.</p>

Values x:x:x:x:x:x:x (eight 16-bit pieces)

telnet-server

Syntax [no] telnet-server

Context config>system>security

Description This command enables Telnet servers running on the system. Telnet servers are off by default. At system startup, only SSH servers are enabled. Telnet servers in networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries. The **no** form of the command disables Telnet servers running on the system.

Login, Telnet, SSH and FTP Commands

exponential-backoff

Syntax	[no] exponential-backoff
Context	config>system>login-control
Description	This command enables the exponential-backoff of the login prompt. The exponential-backoff command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try admin with any conceivable password. The no form of the command disables exponential-backoff.
Default	no exponential-backoff

ftp

Syntax	ftp
Context	config>system>login-control
Description	This command creates the context to configure FTP login control parameters.

idle-timeout

Syntax	idle-timeout {minutes disable} no idle-timeout
Context	config>system>login-control
Description	This command configures the idle timeout for FTP, console, or Telnet sessions before the session is terminated by the system. By default, an idle FTP, console, SSH or Telnet session times out after 30 minutes of inactivity. This timer can be set per session. The no form of the command reverts to the default value.
Default	30 — Idle timeout set for 30 minutes.
Parameters	<i>minutes</i> — The idle timeout in minutes. Allowed values are 1 to 1440. 0 implies the sessions never timeout. Values 1 — 1440 disable — When the disable option is specified, a session will never timeout. To re-enable idle timeout, enter the command without the disable option.

inbound-max-sessions

Syntax	inbound-max-sessions <i>value</i> no inbound-max-sessions
Context	config>system>login-control>ftp
Description	This command configures the maximum number of concurrent inbound FTP sessions. This value is the combined total of inbound and outbound sessions. The no form of the command reverts to the default value.
Default	3
Parameters	<i>value</i> — The maximum number of concurrent FTP sessions on the node. Values 0 — 5

inbound-max-sessions

Syntax	inbound-max-sessions <i>value</i> no inbound-max-sessions
Context	config>system>login-control>telnet
Description	This parameter limits the number of inbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established to the router. The local serial port cannot be disabled. The no form of the command reverts to the default value.
Default	5
Parameters	<i>value</i> — The maximum number of concurrent inbound Telnet sessions, expressed as an integer. Values 0 — 7

login-banner

Syntax	[no] login-banner
Context	config>system>login-control
Description	This command enables or disables the display of a login banner. The login banner contains the 7210 SAS OS copyright and build date information for a console login attempt. The no form of the command causes only the configured pre-login-message and a generic login prompt to display.

login-control

Syntax	login-control
Context	config>system
Description	This command creates the context to configure the session control for console, Telnet and FTP.

motd

Syntax	motd { <i>url url-prefix: source-url</i> text <i>motd-text-string</i> } no motd
Context	config>system>login-control
Description	This command creates the message of the day displayed after a successful console login. Only one message can be configured. The no form of the command removes the message.
Default	No motd is defined.
Parameters	url <i>url-prefix: source-url</i> — When the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote. text <i>motd-text-string</i> — The text of the message of the day. The <i>motd-text-string</i> must be enclosed in double quotes. Multiple text strings are not appended to one another. Some special characters can be used to format the message text. The “\n” character creates multi-line MOTDs and the “\r” character restarts at the beginning of the new line. For example, entering “\n\r” will start the string at the beginning of the new line, while entering “\n” will start the second line below the last character from the first line.

outbound-max-sessions

Syntax	outbound-max-sessions <i>value</i> no outbound-max-sessions
Context	config>system>login-control>telnet
Description	This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled. The no form of the command reverts to the default value.
Default	5
Parameters	<i>value</i> — The maximum number of concurrent outbound Telnet sessions, expressed as an integer. Values 0 — 7

pre-login-message

Syntax	pre-login-message <i>login-text-string</i> [name] no pre-login-message
Context	config>system>login-control
Description	<p>This command creates a message displayed prior to console login attempts on the console via Telnet. Only one message can be configured. If multiple pre-login-messages are configured, the last message entered overwrites the previous entry.</p> <p>It is possible to add the name parameter to an existing message without affecting the current pre-login-message.</p> <p>The no form of the command removes the message.</p>
Default	No pre-login-message is defined.
Parameters	<p><i>login-text-string</i> — The string can be up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>name — When the keyword <i>name</i> is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.</p>

ssh

Syntax	ssh
Context	config>system>login-control
Description	This command enables the context to configure the SSH parameters.

disable-graceful-shutdown

Syntax	[no] disable-graceful-shutdown
Context	config>system>login-control>ssh
Description	<p>This command enables graceful shutdown of SSH sessions.</p> <p>The no form of the command disables graceful shutdown of SSH sessions.</p>

preserve-key

Syntax	[no] preserve-key
Context	config>system>security>ssh
Description	<p>After enabling this command, private keys, public keys, and host key file will be saved by the server. It is restored following a system reboot or the ssh server restart.</p> <p>The no form of the command specifies that the keys will be held in memory by the SSH server and is not restored following a system reboot.</p>
Default	no preserve-key

server-shutdown

Syntax	[no] server-shutdown
Context	config>system>security>ssh
Description	This command enables the SSH servers running on the system.
Default	At system startup, only the SSH server is enabled.

version

Syntax	version ssh-version no version
Context	config>system>security>ssh
Description	Specifies the SSH protocol version that will be supported by the SSH server.
Default	2
Parameters	<i>ssh-version</i> — Specifies the SSH version.
Values	<p>1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1</p> <p>2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2</p> <p>1-2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 1, or SSH protocol version 2 or both.</p>

telnet

- Syntax** `telnet`
- Context** `config>system>login-control`
- Description** This command creates the context to configure the Telnet login control parameters.

enable-graceful-shutdown

- Syntax** `[no] enable-graceful-shutdown`
- Context** `config>system>login-control>telnet`
- Description** This command enables graceful shutdown of telnet sessions.
The no form of the command disables graceful shutdown of telnet sessions.

Management Access Filter Commands

management-access-filter

Syntax	<code>[no] management-access-filter</code>
Context	<code>config>system>security</code>
Description	<p>This command creates the context to edit management access filters and to reset match criteria.</p> <p>Management access filters control all traffic in and out. They can be used to restrict management of the router by other nodes outside either specific (sub)networks or through designated ports.</p> <p>Management filters, as opposed to other traffic filters, are enforced by system software.</p> <p>The no form of the command removes management access filters from the configuration.</p>
Default	No management access filters are defined.

ip-filter

Syntax	<code>[no] ip-filter</code>
Context	<code>config>system>security>mgmt-access-filter</code>
Description	This command enables the context to configure management access IP filter parameters.

ipv6-filter

Syntax	<code>[no] ipv6-filter</code>
Context	<code>config>system>security>mgmt-access-filter</code>
Description	<p>NOTE: On 7210 SAS-Sx IPv6 criteria for Management Access Filters is not supported.</p> <p>This command enables the context to configure management access IPv6 filter parameters.</p>

default-action

Syntax	<code>default-action {permit deny deny-host-unreachable}</code>
Context	<code>config>system>security>mgmt-access-filter>ip-filter</code> <code>config>system>security>mgmt-access-filter>ipv6-filter</code>

Configuration Commands

Description	<p>This command creates the default action for management access in the absence of a specific management access filter match.</p> <p>The default-action is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the default-action must be defined.</p>
Default	No default-action is defined.
Parameters	<p>permit — Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.</p> <p>deny — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued..</p> <p>deny-host-unreachable — Specifies that packets not matching the selection criteria be denied and a host unreachable message will be issued.</p>

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>system>security>mgmt-access-filter>ip-filter config>system>security>mgmt-access-filter>ipv6-filter
Description	<p>This command is used to create or edit a management access filter entry. Multiple entries can be created with unique <i>entry-id</i> numbers. The 7210 SAS OS exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action defined to be considered complete. Entries without the action keyword are considered incomplete and inactive.</p> <p>The no form of the command removes the specified entry from the management access filter.</p>
Default	No entries are defined.
Parameters	<p><i>entry-id</i> — An entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries are numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.</p> <p>Values 1 — 9999</p>

action

Syntax	action { permit deny deny-host-unreachable } no action
Context	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry

- Description** This command creates the action associated with the management access filter match criteria entry. The **action** keyword is required. If no **action** is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.
- If the packet does not meet any of the match criteria the configured **default action** is applied.
- Default** none — The action is specified by default-action command.
- Parameters** *permit* — Specifies that packets matching the configured criteria will be permitted.
- deny** — Specifies that packets matching the configured selection criteria will be denied and that a ICMP host unreachable message will not be issued.
- deny-host-unreachable** — Specifies that packets matching the configured selection criteria will be denied and that a host unreachable message will not be issued.

dst-port

- Syntax** **[no] dst-port port [mask]**
- Context** config>system>security>mgmt-access-filter>ip-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry
- Description** This command configures a source TCP or UDP port number or port range for a management access filter match criterion.
- The **no** form of the command removes the source port match criterion.
- Default** No dst-port match criterion.
- Parameters** *port* — The source TCP or UDP port number as match criteria.

Values 1 — 65535 (decimal)

mask — Mask used to specify a range of source port numbers as the match criterion.

This 16 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0BBBBBBBBBBBBBBBB	0b1111100000000000

To select a range from 1024 up to 2047, specify 1024 0xFC00 for value and mask.

Default 65535 (exact match)

Values 1 — 65535 (decimal)

fragment

Syntax	[no] fragment {true false}
Context	config>system>security>mgmt-access-filter>ip-filter>ip-filter>entry
Description	<p>Platforms Supported: 7 This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion.</p> <p>Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.</p> <p>The no form of the command removes the match criterion.</p>
Default	no fragment
Parameters	<p><i>true</i> — Specifies to match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.</p> <p><i>false</i> — Specifies to match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.</p>

I4-src-port

Syntax	[no] I4-src-port port [mask]
Context	config>system>security>mgmt-access-filter>ip-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry
Description	<p>This command configures a source TCP or UDP port number for an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.</p> <p>The no form of the command removes the source port match criterion.</p>
Default	no I4-src-port
Parameters	<p><i>port</i> — The source port number to be used as a match criteria expressed as a decimal integer.</p> <p>Values [1..65535]</p> <p><i>mask</i> — Specifies the mask in dotted decimal notation</p> <p>Values [1..65535]decimal hex or binary</p>

flow-label

Syntax	flow-label value no flow-label
Context	config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as nondefault quality of service or real-time service.

Parameters *value* — Specify the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, Textual Conventions for IPv6 Flow Label.)

Values 0 — 1048575

log

Syntax [no] log

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command enables match logging. When enabled, matches on this entry will cause the Security event mafEntryMatch to be raised.

Default no log

next-header

Syntax **next-header** *next-header*
no next-header

Context config>system>security>mgmt-access-filter>ipv6-filter>entry

Description This command specifies the next header to match. The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).

Parameters *next-header* — Specifies for IPv4 MAF the IP protocol field, and for IPv6 the next header type to be used in the match criteria for this Management Access Filter Entry.

Values next-header: 0 — 255, protocol numbers accepted in DHB
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

protocol

Syntax [no] **protocol** *protocol-id*

Configuration Commands

Context	config>system>security>mgmt-access-filter>ip-filter>entry
Description	<p>This command configures an IP protocol type to be used as a management access filter match criterion.</p> <p>The protocol type, such as TCP, UDP, and OSPF, is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).</p> <p>The no form of the command removes the protocol from the match criteria.</p>
Default	No protocol match criterion is specified.
Parameters	<i>protocol</i> — The protocol number for the match criterion.
Values	1 - 255 (decimal)

router

Syntax	router { <i>router-instance</i> } no router
Context	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry
Description	<p>The command configures a router name or service ID to be used as a management access filter match criterion.</p> <p>The no form of the command removes the router name or service ID from the match criteria.</p>
Default	Base
Parameters	<i>router-instance</i> — Specifies the router name.
Values	Base, Management (Applicable to 7210 SAS devices configured in Network mode)
Values	Base, Management, vpls-management (for 7210 SAS-M and SAS-T devices configured in access uplink mode)

renum

Syntax	renum <i>old-entry-number new-entry-number</i>
Context	config>system>security>mgmt-access-filter>ip-filter config>system>security>mgmt-access-filter>ipv6-filter
Description	<p>This command renumbers existing management access filter entries to re-sequence filter entries.</p> <p>The exits on the first match found and executes the actions in accordance with the accompanying action command. This may require some entries to be re-numbered differently from most to least explicit.</p>
Parameters	<i>old-entry-number</i> — Enter the entry number of the existing entry.
Values	1 — 9999

new-entry-number — Enter the new entry number that will replace the old entry number.

Values 1 — 9999

match

Syntax	match [frame-type <i>frame-type</i>] no match
Context	config>system>security>mgmt-access-filter>mac-filter>entry config>system>security>cpm-filter>mac-filter>entry
Description	This command configures math criteria for this MAC filter entry.
Parameters	frame-type <i>frame-type</i> — Specifies the type of MAC frame to use as match criteria. Values none, 802dot2-llc, ethernet_II Values

src-port

Syntax	src-port { <i>port-id</i> lag <i>lag-id</i> } no src-port
Context	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry
Description	This command restricts ingress management traffic to either the CPM Ethernet port or any other logical port (LAG or port) on the device. When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria. The no form of the command reverts to the default value.
Default	any interface
Parameters	<i>port-id</i> — The port ID in the following format: slot[/mda]/port. Syntax: port-id: slot/mda/port

src-ip

Syntax	[no] src-ip { ip-prefix/prefix-length <ip-prefix> <netmask> }
Context	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry

Configuration Commands

Description	<p>This command configures a source IP address range to be used as a management access filter match criterion.</p> <p>To match on the source IP address, specify the address and the associated mask (that is, 10.1.0.0/16). The conventional notation of 10.1.0.0 255.255.0.0 can also be used.</p> <p>The no form of the command removes the source IP address match criterion.</p>
Default	No source IP match criterion is specified.
Parameters	<p><i>ip-prefix/prefix-length</i> — The IP prefix used for IP match criteria in dotted decimal notation. Can be IPv4 or an IPv6 prefix.</p> <p>ipv4-prefix: a.b.c.d</p> <p>ipv4-prefix-length: 0 — 32</p> <p>ipv6-prefix: x:x:x:x:x:x:x (eight 16-bit pieces)</p> <p>x:x:x:x:x:d.d.d.d</p> <p>x: [0..FFFF]H</p> <p>d: [0..255]D</p> <p>ipv6-prefix-length: 0 — 128</p> <p><i>netmask</i> — Specifies the subnet mask in dotted decimal notation.</p> <p>Values 0.0.0.0 - 255.255.255.255</p>

IPsec Command Reference

ipsec

Syntax	ipsec
Context	config
Description	This command enables the context to configure Internet Protocol security (IPSec) parameters. IPSec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

static-sa

Syntax	static-sa <i>sa-name</i> no static-sa
Context	config>ipsec
Description	This command configures an IPsec static SA.

authentication

Syntax	authentication { md5 <i>key-1</i> sha <i>key-1</i> } privacy <i>privacy-level</i> <i>key-2</i> [hash] no authentication
Context	config>ipsec>static-sa
Description	This command configures the authentication algorithm to use for an IPsec manual SA. The no statement resets to the default value.
Default	sha1
Parameters	<p>ascii-key — Specifies an ASCII key.</p> <p>hex-key — Specifies a HEX key.</p> <p>hash — When hash is not specified, then non-encrypted characters can be entered. When hash is configured, then all specified keys are stored in an encrypted format in the configuration file. The password must be entered in encrypted form when the hash parameter is used.</p> <p>md5 <i>key</i> — The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.</p> <p>The MD5 authentication key is stored in an encrypted format. The minimum key length is determined by the config>system>security>password>minimum-length value. The maximum length is 16 octets (32 printable characters).</p> <p>The complexity of the key is determined by the complexity command.</p>

Configuration Commands

sha *key* — The authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96.

The **sha** authentication key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 20 octets (40 printable characters).

The complexity of the key is determined by the **complexity** command.

privacy none — Do not perform SNMP packet encryption.

Default privacy none

description

Syntax	description <i>description-string</i> no description
Context	config>ipsec>static-sa
Description	This command creates a text description which is stored in the configuration file to help identify the content of the entity. The no form of the command removes the string from the configuration.
Default	none
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.

direction

Syntax	direction <i>inbound outbound bidirectional</i> no direction
Context	config>ipsec>static-sa
Description	This command configures the direction for an IPsec manual SA. The no statement resets to the default value.
Default	bidirectional

protocol

Syntax	protocol <i>ah esp</i> no protocol
Context	config>ipsec>static-sa

Description This command configures the security protocol to use for an IPsec manual SA. The no statement resets to the default value.

Default esp

Parameters *ah* — Specifies the Authentication Header protocol.
esp — Specifies the Encapsulation Security Payload protocol.

spi

Syntax **spi** *spi-key*
no spi

Context config>ipsec>static-sa

Description This command configures the SPI key value for an IPsec manual SA. The no statement resets to the default value.

Password Commands

admin-password

Syntax	admin-password <i>password</i> [hash hash2] no admin-password
Context	config>system>security>password
Description	<p>This command allows a user (with admin permissions) to configure a password which enables a user to become an administrator.</p> <p>This password is valid only for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.</p> <p>This functionality can be enabled in two contexts:</p> <pre>config>system>security>password>admin-password <global> enable-admin</pre> <p>NOTE: See the description for the enable-admin on the next page. If the admin-password is configured in the config>system>security>password context, then any user can enter the special mode by entering the enable-admin command.</p> <p>enable-admin is in the default profile. By default, all users are given access to this command.</p> <p>Once the enable-admin command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.</p> <p>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.</p> <p>NOTE: The <i>password</i> argument of this command is not sent to the servers. This is consistent with other commands which configure secrets.</p> <p>Also note that usernames and passwords in the FTP and TFTP URLs will not be sent to the authorization or accounting servers when the file>copy source-url dest-url command is executed.</p> <p>For example:</p> <pre>file copy ftp://test:secret@131.12.31.79/test/srcfile cf1:\destfile</pre> <p>In this example, the username 'test' and password 'secret' will not be sent to the AAA servers (or to any logs). They will be replaced with '****'.</p> <p>The no form of the command removes the admin password from the configuration.</p>
Default	no admin-password
Parameters	<p><i>password</i> — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.</p> <p>hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted</p>

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

enable-admin

Syntax	enable-admin
Context	<global>
Description	<p>NOTE: See the description for the admin-password on the previous page. If the admin-password is configured in the <code>config>system>security>password</code> context, then any user can enter the special administrative mode by entering the enable-admin command.</p> <p>enable-admin is in the default profile. By default, all users are given access to this command.</p> <p>Once the enable-admin command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.</p> <p>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.</p> <p>There are two ways to verify that a user is in the enable-admin mode:</p> <ul style="list-style-type: none"> • <code>show users</code> – Administrator can know which users are in this mode. • Enter the <code>enable-admin</code> 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 09AUG2006 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#
```

aging

Syntax	aging <i>days</i> no aging
Context	config>system>security>password
Description	This command configures the number of days a user password is valid before the user must change their password. This parameter can be used to force the user to change the password at the configured interval. The no form of the command reverts to the default value.
Default	No aging is enforced.
Parameters	<i>days</i> — The maximum number of days the password is valid. Values 1 — 500

attempts

Syntax	attempts <i>count</i> [time <i>minutes1</i> [lockout <i>minutes2</i>]] no attempts
Context	config>system>security>password
Description	This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame. The threshold for the number of login attempts can be configured by using the CLI parameter ' count ' in the command. A SNMP trap is generated by the device, when the number of login attempts exceeds the configured threshold. Generation of the trap can be suppressed, by using the config>log> event-control command. By default, the device generates a trap when the login attempts exceed the configured threshold. The trap carries information about the user ID used for the login attempt. A SNMP trap will not be sent for every failed attempt. If the threshold is exceeded, the user is locked out for a specified time period. If multiple attempts commands are entered, each command overwrites the previously entered command. The no attempts command resets all values to default.
Default	count: 3 time <i>minutes: 5</i> lockout <i>minutes: 10</i>
Parameters	<i>count</i> — The number of unsuccessful login attempts allowed for the specified time . This is a mandatory value that must be explicitly entered. Values 1 — 64

time *minutes* — The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.

Values 0 — 60

lockout *minutes* — The lockout period in minutes where the user is not allowed to login. Allowed values are decimal integers.

Values 0 — 1440

When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period.

Default 10

Values 0 — 1440

authentication-order

Syntax	authentication-order [<i>method-1</i>] [<i>method-2</i>] [<i>method-3</i>] [exit-on-reject] no authentication-order
Context	config>system>security>password
Description	<p>This command configures the sequence in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.</p> <p>The order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.</p> <p>If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log register the failed attempt. Both the attempted login identification and originating IP address is logged with the a timestamp.</p> <p>The no form of the command reverts to the default authentication sequence.</p>
Default	authentication-order radius tacplus local - The preferred order for password authentication is 1. RADIUS, 2. TACACS+ and 3. local passwords.
Parameters	<p><i>method-1</i> — The first password authentication method to attempt.</p> <p>Default radius</p> <p>Values radius, tacplus, local</p> <p><i>method-2</i> — The second password authentication method to attempt.</p> <p>Default tacplus</p> <p>Values radius, tacplus, local</p> <p><i>method-3</i> — The third password authentication method to attempt.</p> <p>Default local</p> <p>Values radius, tacplus, local</p>

radius — RADIUS authentication.

tacplus — TACACS+ authentication.

local — Password authentication based on the local password database.

exit-on-reject — When enabled and if one of the AAA methods configured in the authentication order sends a reject, then the next method in the order will not be tried. If the **exit-on-reject** keyword is not specified and if one AAA method sends a reject, the next AAA method will be attempted. If in this process, all the AAA methods are exhausted, it will be considered as a reject.

Note that a rejection is distinct from an unreachable authentication server. When the **exit-on-reject** keyword is specified, authorization and accounting will only use the method that provided an affirmation authentication; only if that method is no longer readable or is removed from the configuration will other configured methods be attempted. If the local keyword is the first authentication and:

- **exit-on-reject** is configured and the user does not exist, the user will not be authenticated.
- The user is authenticated locally, then other methods, if configured, will be used for authorization and accounting.
- The user is configured locally but without console access, login will be denied.

complexity

Syntax	[no] complexity [numeric] [special-character] [mixed-case]
Context	config>system>security>password
Description	<p>This command configures the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and des-keys configured in the authentication section.</p> <p>If more than one complexity command is entered, each command overwrites the previous command.</p> <p>The no form of the command cancels all requirements. To remove a single requirement, enter the no form of the command followed by the requirement that needs to be removed.</p> <p>For example, no complexity numeric.</p>
Default	No complexity requirements are configured.
Parameters	<p>mixed-case — Specifies that at least one upper and one lower case character must be present in the password. This keyword can be used in conjunction with the numeric and special-character parameters. However, if this command is used with the authentication none command, the complexity command is rejected.</p> <p>numeric — Specifies that at least one numeric character must be present in the password. This keyword can be used in conjunction with the mixed-case and special-character parameters. However, if this command is used with the authentication none command, the complexity command is rejected.</p> <p>special-character — Specifies that at least one special character must be present in the password. This keyword can be used in conjunction with the numeric and special-character parameters.</p>

However, if this command is used with the **authentication none** command, the **complexity** command is rejected.

Special characters include: ~!@#\$\$%^&*()_+{|}:”<>?”-=[\];’,./.

health-check

Syntax	[no] health-check [interval <i>interval</i>]
Context	config>system>security>password
Description	This command specifies that RADIUS and TACACS+ servers are monitored for 3 seconds each at 30 second intervals. Servers that are not configured will have 3 seconds of idle time. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent. The no form of the command disables the periodic monitoring of the RADIUS and TACACS+ servers. In this case, the operational status for the active server will be up if the last access was successful.
Default	health-check
Parameters	<i>interval</i> — Specifies the interval of the health check in seconds. Values 6 — 1500

minimum-length

Syntax	minimum-length <i>value</i> no minimum-length
Context	config>system>security>password
Description	This command configures the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the system security section. If multiple minimum-length commands are entered each command overwrites the previous entered command. The no form of the command reverts to default value.
Default	minimum-length 6
Parameters	<i>value</i> — The minimum number of characters required for a password. Values 1 — 8

password

Syntax	password
---------------	-----------------

Configuration Commands

Context config>system>security

Description This command creates the context to configure password management parameters.

Profile Management Commands

action

Syntax	action {deny permit}
Context	config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
Description	This command configures the action associated with the profile entry.
Parameters	deny — Specifies that commands matching the entry command match criteria are to be denied. permit — Specifies that commands matching the entry command match criteria will be permitted.

match

Syntax	match <i>command-string</i> no match
Context	config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
Description	This command configures a command or subtree commands in subordinate command levels are specified. Because the exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile. All commands below the hierarchy level of the matched command are denied. The no form of this command removes a match condition
Default	none
Parameters	<i>command-string</i> — The CLI command or CLI tree level that is the scope of the profile entry.

copy

Syntax	copy { user <i>source-user</i> profile <i>source-profile</i> } to <i>destination</i> [overwrite]
Context	config>system>security
Description	This command copies a profile or user from a source profile to a destination profile.
Parameters	<i>source-profile</i> — The profile to copy. The profile must exist. <i>dest-profile</i> — The copied profile is copied to the destination profile.

Configuration Commands

overwrite — Specifies that the destination profile configuration will be overwritten with the copied source profile configuration. A profile will not be overwritten if the **overwrite** command is not specified.

default-action

Syntax	default-action { deny-all permit-all none }
Context	config>system>security>profile <i>user-profile-name</i>
Description	This command specifies the default action to be applied when no match conditions are met.
Default	none
Parameters	deny-all — Sets the default of the profile to deny access to all commands. permit-all — Sets the default of the profile to permit access to all commands. Note: permit-all does not change access to security commands. Security commands are only and always available to members of the super-user profile. none — Sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user. For example, if a user is a member of two profiles and the default action of the first profile is permit-all , then the second profile will never be evaluated because the permit-all is executed first. Set the first profile default action to none and if no match conditions are met in the first profile, then the second profile will be evaluated. If the default action of the last profile is none and no explicit match is found, then the default deny-all takes effect.

description

Syntax	description <i>description-string</i> no description
Context	config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
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 context in the configuration file. The no form of the command removes the string from the context.
Default	No description is configured.
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.

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>system>security>profile <i>user-profile-name</i>
Description	<p>This command is used to create a user profile entry.</p> <p>More than one entry can be created with unique <i>entry-id</i> numbers. Exits when the first match is found and executes the actions according to the accompanying action command. Entries should be sequenced from most explicit to least explicit.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete.</p> <p>The no form of the command removes the specified entry from the user profile.</p>
Default	No entry IDs are defined.
Parameters	<p><i>entry-id</i> — An entry-id uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the <i>entry-ids</i> should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.</p> <p>Values 1 — 9999</p>

profile

Syntax	[no] profile <i>user-profile-name</i>
Context	config>system>security
Description	<p>This command creates a context to create user profiles for CLI command tree permissions.</p> <p>Profiles are used to either deny or permit user console access to a hierarchical branch or to specific commands.</p> <p>Once the profiles are created, the users command assigns users to one or more profiles. You can define up to 16 user profiles but a maximum of 8 profiles can be assigned to a user. The <i>user-profile-name</i> can consist of up to 32 alphanumeric characters.</p> <p>The no form of the command deletes a user profile.</p>
Default	user-profile default
Parameters	<p><i>user-profile-name</i> — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.</p>

renum

Syntax	renum <i>old-entry-number new-entry-number</i>
Context	config>system>security>profile <i>user-profile-name</i>

Configuration Commands

Description This command renumbers profile entries to re-sequence the entries.
Since the exits when the first match is found and executes the actions according to accompanying action command, re-numbering is useful to rearrange the entries from most explicit to least explicit.

Parameters *old-entry-number* — Enter the entry number of an existing entry.

Values 1 — 9999

new-entry-number — Enter the new entry number.

Values 1 — 9999

User Management Commands

access

Syntax	<code>[no] access [ftp] [snmp] [console]</code>
Context	config>system>security>user config>system>security>user-template
Description	<p>This command grants a user permission for FTP, SNMP, console or lawful intercept (LI) access.</p> <p>If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated additively.</p> <p>The no form of command removes access for a specific application.</p> <p>no access denies permission for all management access methods. To deny a single access method, enter the no form of the command followed by the method to be denied, for example, no access FTP denies FTP access.</p>
Default	No access is granted to the user by default.
Parameters	<p>ftp — Specifies FTP permission.</p> <p>snmp — Specifies SNMP permission. This keyword is only configurable in the <code>config>system>security>user</code> context.</p> <p>console — Specifies console access (serial port or Telnet) permission.</p>

authentication

Syntax	<code>authentication {[none] [[hash] {md5 key-1 sha key-1} privacy {privacy-level key-2}]}</code>
Context	config>system>security>user>snmp
Description	<p>This command configures the authentication and encryption method the user must use in order to be validated by the device. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered.</p> <p>The user password is encrypted first by the MD5/SHA/DES algorithm. The output of the algorithm is always a fixed length string (key). Copy the password key and paste the output in the appropriate authentication command <i>key</i> parameter.</p>
Default	authentication none - No authentication is configured and privacy cannot be configured.
Parameters	<p>none — Do not use authentication. If none is specified, then privacy cannot be configured.</p> <p>hash — When hash is not specified, then non-encrypted characters can be entered. When hash is configured, then all specified keys are stored in an encrypted format in the configuration file. The password must be entered in encrypted form when the hash parameter is used.</p> <p>md5 key — The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.</p>

Configuration Commands

The MD5 authentication key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 16 octets (32 printable characters).

The complexity of the key is determined by the **complexity** command.

sha key — The authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96.

The **sha** authentication key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 20 octets (40 printable characters).

The complexity of the key is determined by the **complexity** command.

privacy none — Do not perform SNMP packet encryption.

Default **privacy none**

privacy des-key key — Configure the **des-key** for SNMP packet encryption. This key is stored in an encrypted format. The minimum key length is determined by the **config>system>security>password>minimum-length** value. The maximum length is 16 octets (32 printable characters). If privacy is configured then **authentication** must be enabled.

To remove a previously configured **des-key**, enter **privacy none**.

The complexity of the key is determined by the **complexity** command.

Default **privacy none**

group

Syntax	group <i>group-name</i> no group
Context	config>system>security>user>snmp
Description	This command associates (or links) a user to a group name. The group name must be configured with the config>system>security>user >snmp>group command. The access command links the group with one or more views, security model (s), security level (s), and read, write, and notify permissions
Default	No group name is associated with a user.
Parameters	<i>group-name</i> — Enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group-name per security model.

cannot-change-password

Syntax	[no] cannot-change-password
Context	config>system>security>user>console
Description	This command allows a user the privilege to change their password for both FTP and console login. To disable a user's privilege to change their password, use the cannot-change-password form of the command. Note that the cannot-change-password flag is not replicated when a user copy is performed. A new-password-at-login flag is created instead.
Default	no cannot-change-password

console

Syntax	console
Context	config>system>security>user config>system>security>user-template
Description	This command creates the context to configure user profile membership for the console (either Telnet or serial port user).

copy

Syntax	copy {user <i>source-user</i> profile <i>source-profile</i>} to <i>destination</i> [overwrite]
Context	config>system>security
Description	This command copies a specific user's configuration parameters to another (destination) user. The password is set to a carriage return and a new password at login must be selected.
Parameters	<i>source-user</i> — The user to copy. The user must already exist. <i>dest-user</i> — The copied profile is copied to a destination user. overwrite — Specifies that the destination user configuration will be overwritten with the copied source user configuration. A configuration will not be overwritten if the overwrite command is not specified.

home-directory

Syntax	home-directory <i>url-prefix</i> [<i>directory</i>] [<i>directory</i>/<i>directory</i>...]
---------------	---

Configuration Commands

no home-directory

Context	config>system>security>user config>system>security>user-template
Description	This command configures the local home directory for the user for both console and FTP access. If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed. The no form of the command removes the configured home directory.
Default	no home-directory NOTE: If restrict-to-home has been configured no file access is granted and no home-directory is created, if restrict-to-home is not applied then root becomes the user's home-directory.
Parameters	<i>local-url-prefix</i> [<i>directory</i>] [<i>directory/directory...</i>] — The user's local home directory URL prefix and directory structure up to 190 characters in length.

profile

Syntax	profile <i>user-profile-name</i> no profile
Context	config>system>security>user-template
Description	This command configures the profile for the user based on this template.
Parameters	<i>user-profile-name</i> — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

login-exec

Syntax	[no] login-exec <i>url-prefix: source-url</i>
Context	config>system>security>user>console config>system>security>user-template>console
Description	This command configures a user's login exec file which executes whenever the user successfully logs in to a console session. Only one exec file can be configured. If multiple login-exec commands are entered for the same user, each subsequent entry overwrites the previous entry. The no form of the command disables the login exec file for the user.
Default	No login exec file is defined.
Parameters	<i>url-prefix: source-url</i> — Enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that will be executed after the user successfully logs in.

member

Syntax	member <i>user-profile-name</i> [<i>user-profile-name...up to 8max</i>] no member <i>user-profile-name</i>
Context	config>system>security>user>console
Description	This command is used to allow the user access to a profile. A user can participate in up to eight profiles. The no form of this command deletes access user access to a profile.
Default	default
Parameters	<i>user-profile-name</i> — The user profile name.

new-password-at-login

Syntax	[no] new-password-at-login
Context	config>system>security>user>console
Description	This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login. The no form of the command does not force the user to change passwords.
Default	no new-password-at-login

password

Syntax	password [<i>password</i>] [hash hash2]
Context	config>system>security>user
Description	This command configures the user password for console and FTP access. The use of the hash keyword sets the initial password when the user is created or modifies the password of an existing user and specifies that the given password was hashed using hashing algorithm version 1. The password is stored in an encrypted format in the configuration file when specified. Passwords should be encased in double quotes (" ") at the time of the password creation. The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string. The use of the hash2 keyword specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify if it is a valid hash 2 key to store in the database. For example, <pre>config>system>security# user testuser1 config>system>security>user\$ password "zx/Uhcn6ReMOZ3BVrWcvk." hash2</pre>

Configuration Commands

```
config>system>security>user# exit

config>system>security# info
-----
...
        user "testuser1"
            password "zx/Uhcn6ReMOZ3BvrWcvk." hash2
        exit
...
-----
config>system>security#
```

Parameters

password — This is the password for the user that must be entered by this user during the login procedure. The minimum length of the password is determined by the **minimum-length** command. The maximum length can be up to 20 chars if unhashed, 32 characters if hashed. The complexity requirements for the password is determined by the **complexity** command.

All password special characters (#, \$, spaces, etc.) must be enclosed within double quotes.

For example: config>system>security>user# password "south#bay?"

The question mark character (?) cannot be directly inserted as input during a telnet connection because the character is bound to the **help** command during a normal Telnet/console connection.

To insert a # or ? characters, they must be entered inside a notepad or clipboard program and then cut and pasted into the Telnet session in the password field that is encased in the double quotes as delimiters for the password.

If a password is entered without any parameters, a password length of zero is implied: (carriage return).

hash — Specifies that the given password is already hashed using hashing algorithm version 1. A semantic check is performed on the given password field to verify if it is a valid hash 1 key to store in the database.

hash2 — Specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify if it is a valid hash 2 key to store in the database.

restricted-to-home

Syntax [no] restricted-to-home

Context config>system>security>user
config>system>security>user-template

Description This command prevents users from navigating above their home directories for file access. A user is not allowed to navigate to a directory higher in the directory tree on the home directory device. The user is allowed to create and access subdirectories below their home directory.

If a home-directory is not configured or the home directory is not available, then the user has no file access.

The **no** form of the command allows the user access to navigate to directories above their home directory.

Default no restricted-to-home

snmp

Syntax **snmp**

Context config>system>security>user

Description This command creates the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters.

All SNMPv3 users must be configured with the commands available in this CLI node.

always uses the configured SNMPv3 user name as the security user name.

user-template

Syntax **user-template {tacplus_default | radius_default}**

Context config>system>security

Description This command configures default security user template parameters.

Parameters **tacplus_default** — Specifies that the default TACACS+ user template is actively applied to the TACACS+ user.

radius_default — specifies that the default RADIUS user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server.

users

Syntax **users**

Context show

Description This command creates a local user and a context to edit the user configuration.

When creating a new user and then entering the **info** command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that user name, there will be no password required. The user can login to the system and then <ENTER> at the password prompt, the user will be logged in.

Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the username and null password field, so when the username is changed, the displayed hashed value will change.

Default none

user

Syntax	user <i>user-name</i>
Context	admin
Description	<p>This command creates a local user and a context to edit the user configuration.</p> <p>If a new <i>user-name</i> is entered, the user is created. When an existing <i>user-name</i> is specified, the user parameters can be edited.</p> <p>When creating a new user and then entering the info command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that user name, there will be no password required. The user can login to the system and then <ENTER> at the password prompt, the user will be logged in.</p> <p>Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the username and null password field, so when the username is changed, the displayed hashed value will change.</p> <p>The no form of the command deletes the user and all configuration data. Users cannot delete themselves.</p>
Default	none
Parameters	<i>user-name</i> — The name of the user up to 16 characters.

RADIUS Client Commands

accounting

Syntax	[no] accounting
Context	config>system>security>radius
Description	This command enables RADIUS accounting. The no form of this command disables RADIUS accounting.
Default	no accounting

accounting-port

Syntax	accounting-port <i>port</i> no accounting-port
Context	config>system>security>radius
Description	This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.
Parameters	<i>port</i> — Specifies the UDP port number.
Values	1 — 65535
Default	1813

authorization

Syntax	[no] authorization
Context	config>system>security>radius
Description	This command configures RADIUS authorization parameters for the system.
Default	no authorization

port

Syntax	port <i>port</i> no port
Context	config>system>security>radius

Configuration Commands

Description	This command configures the TCP port number to contact the RADIUS server. The no form of the command reverts to the default value.
Default	1812 (as specified in RFC 2865, <i>Remote Authentication Dial In User Service (RADIUS)</i>)
Parameters	<i>port</i> — The TCP port number to contact the RADIUS server. Values 1 — 65535

radius

Syntax	[no] radius
Context	config>system>security
Description	This command creates the context to configure RADIUS authentication on the router. Implement redundancy by configuring multiple server addresses for each router. The no form of the command removes the RADIUS configuration.

retry

Syntax	retry count no retry
Context	config>system>security>radius config>system>security>dot1x>radius-plcy
Description	This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server. The no form of the command reverts to the default value.
Default	3
Parameters	<i>count</i> — The retry count. Values 1 — 10

server

Syntax	server server-index address ip-address secret key [hash hash2] [auth-port auth-port] [acct-port acct-port] [type server-type] no server index
Context	config>system>security>radius
Description	This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

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

Default No RADIUS servers are configured.

Parameters *index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 — 5

address *ip-address* — The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values

ipv4-address	a.b.c.d (host bits must be 0)
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

secret *key* — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values Up to 20 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

shutdown

Syntax [no] shutdown

Context config>system>security>radius

Description This command administratively disables the RADIUS protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

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 the command administratively enables the protocol which is the default state.

Default no shutdown

timeout

Syntax	timeout <i>seconds</i> no timeout
Context	config>system>security>radius
Description	This command configures the number of seconds the router waits for a response from a RADIUS server. The no form of the command reverts to the default value.
Default	3 seconds
Parameters	<i>seconds</i> — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer. Values 1 — 90

use-default-template

Syntax	[no] use-default-template
Context	config>system>security>radius
Description	This command specifies whether the RADIUS user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the RADIUS user template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server. The no form of the command disables the command.

TACACS+ Client Commands

server

Syntax	server <i>index</i> address <i>ip-address</i> secret <i>key</i> no server <i>index</i>															
Context	config>system>security>tacplus															
Description	<p>This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.</p> <p>Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.</p> <p>The no form of the command removes the server from the configuration.</p>															
Default	No TACACS+ servers are configured.															
Parameters	<p><i>index</i> — The index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.</p> <p>Values 1 — 5</p> <p>address <i>ip-address</i> — The IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.</p> <table> <tr> <td>Values</td> <td>ipv4-address</td> <td>a.b.c.d (host bits must be 0)</td> </tr> <tr> <td></td> <td>ipv6-address</td> <td>x:x:x:x:x:x:x (eight 16-bit pieces)</td> </tr> <tr> <td></td> <td></td> <td>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> <p>secret <i>key</i> — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.</p> <p>Values Up to 128 characters in length.</p> <p>hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.</p> <p>hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.</p> <p>Values</p>	Values	ipv4-address	a.b.c.d (host bits must be 0)		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
Values	ipv4-address	a.b.c.d (host bits must be 0)														
	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														

shutdown

Syntax [no] shutdown

Configuration Commands

Context config>system>security>tacplus

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

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 the command administratively enables the protocol which is the default state.

Default no shutdown

tacplus

Syntax [no] tacplus

Context config>system>security

Description This command creates the context to configure TACACS+ authentication on the router.

Configure multiple server addresses for each router for redundancy.

The **no** form of the command removes the TACACS+ configuration.

accounting

Syntax accounting [record-type {start-stop | stop-only}]
no accounting

Context config>system>security>tacplus

Description This command configures the type of accounting record packet that is to be sent to the TACACS+ server. The **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent.

Default record-type stop-only

Parameters **record-type start-stop** — Specifies that a TACACS+ start packet is sent whenever the user executes a command.

record-type stop-only — Specifies that a stop packet is sent whenever the command execution is complete.

authorization

Syntax [no] authorization

Context config>system>security>tacplus

Description This command configures TACACS+ authorization parameters for the system.

Default no authorization

timeout

Syntax **timeout** *seconds*
no timeout

Context config>system>security>tacplus

Description This command configures the number of seconds the router waits for a response from a TACACS+ server.

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

Default 3

Parameters *seconds* — The number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 — 90

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>tacplus

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

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 the command administratively enables the protocol which is the default state.

Default no shutdown

use-default-template

Syntax [**no**] **use-default-template**

Context config>system>security>tacplus

Description This command specifies whether or not the user template defined by this entry is to be actively applied to the TACACS+ user.

Generic 802.1x COMMANDS

dot1x

Syntax	[no] dot1x
Context	config>system>security
Description	This command creates the context to configure 802.1x network access control on the 7210 SAS-Series router. The no form of the command removes the 802.1x configuration.

radius-plcy

Syntax	[no] radius-plcy <i>name</i> [create]
Context	config>system>security> dot1x
Description	This command creates the context to configure RADIUS server parameters for 802.1x network access control on the 7210 SAS-Series router. NOTE: The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the 7210 SAS-Series as opposed to the RADIUS server configured under the config>system>radius context which authenticates CLI login users who get access to the management plane of the 7210 SAS-Series. The no form of the command removes the RADIUS server configuration for 802.1x.
Parameters	<i>name</i> — Specifies the name of the RADIUS policy. Values 1 — 32 characters create — This keyword is mandatory to create a RADIUS policy.

retry

Syntax	retry <i>count</i> no retry
Context	config>system>security> dot1x
Description	This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server. The no form of the command reverts to the default value.
Default	3

Parameters *count* — The retry count.

Values 1 — 10

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2**] [**auth-port** *auth-port*] [**acct-port** *acct-port*] [**type** *server-type*]
no server *index*

Context config>system>security> dot1x>radius-plcy

Description This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.

Up to five Dot1x servers can be configured at any one time. Dot1x servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other Dot1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

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

Default No Dot1x servers are configured.

Parameters *server-index* — The index for the Dot1x server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 — 5

address *ip-address* — The IP address of the Dot1x server. Two Dot1x servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret *key* — The secret key to access the Dot1x server. This secret key must match the password on the Dot1x server.

Values secret-key - Up to 20 characters

Values hash-key - Up to 33 characters

Values hash2-key - Up to 55 characters

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

acct-port *acct-port* — The UDP port number on which to contact the RADIUS server for accounting requests.

Values 1 — 65535

Configuration Commands

auth-port *auth-port* — specifies a UDP port number to be used as a match criteria.

Values 1 — 65535

type *server-type* — Specifies the server type.

Values authorization, accounting, combined

source-address

Syntax **source-address** *ip-address*
no source-address

Context config>system>security> dot1x>radius-plcy

Description This command configures the NAS IP address to be sent in the RADIUS packet.
The **no** form of the command reverts to the default value.

Default By default the System IP address is used in the NAS field.

Parameters *ip-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255

shutdown

Syntax [**no**] **shutdown**

Context config>system>security>dot1x
config>system>security>dot1x>radius-plcy

Description This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.
The operational state of the entity is disabled as well as the operational state of any entities contained within.
The **no** form of the command administratively enables the protocol which is the default state.

Default shutdown

timeout

Syntax **timeout** *seconds*
no timeout

Context config>system>security> dot1x>radius-plcy

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

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

Default 3 seconds

Parameters *seconds* — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 — 90

TCP Enhanced Authentication

keychain

Syntax	[no] keychain <i>keychain-name</i>
Context	config>system>security
Description	This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session. The no form of the command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.
Default	none
Parameters	<i>keychain-name</i> — Specifies a keychain name which identifies this particular keychain entry.
Values	An ASCII string up to 32 characters.

direction

Syntax	direction
Context	config>system>security>keychain
Description	This command specifies the data type that indicates the TCP stream direction to apply the keychain.
Default	none

bi

Syntax	bi
Context	config>system>security>keychain>direction
Description	This command configures keys for both send and receive stream directions.
Default	none

uni

Syntax	uni
Context	config>system>security>keychain>direction

Description This command configures keys for send or receive stream directions.

Default none

receive

Syntax **receive**

Context config>system>security>keychain>direction>uni

Description This command enables the receive nodal context. Entries defined under this context are used to authenticate TCP segments that are being received by the router.

Default none

send

Syntax **send**

Context config>system>security>keychain>direction>uni

Description This command specifies the send nodal context to sign TCP segments that are being sent by the router to another device.

Default none

entry

Syntax **entry** *entry-id* **key** [*authentication-key* | *hash-key* | *hash2-key*] [**hash** | **hash2**] **algorithm**
algorithm
no entry *entry-id*

Context config>system>security>keychain>direction>bi
config>system>security>keychain>direction>uni>receive
config>system>security>keychain>direction>uni>send

Description This command defines a particular key in the keychain. Entries are defined by an entry-id. A keychain must have valid entries for the TCP Enhanced Authentication mechanism to work.

The **no** form of the command removes the entry from the keychain. If the entry is the active entry for sending, then this will cause a new active key to be selected (if one is available using the youngest key rule). If it is the **ONLY** possible send key, then the system will reject the command with an error indicating the configured key is the only available send key.

If the key is one of the eligible keys for receiving, it will be removed. If the key is the **ONLY** possible eligible key, then the command will not be accepted, and an error indicating that this is the only eligible key will be output.

The **no** form of the command deletes the entry.

Configuration Commands

Default	There are no default entries.
Parameters	<p><i>entry-id</i> — Specifies an entry that represents a key configuration to be applied to a keychain.</p> <p>Values 0 — 63</p> <p>key — Specifies a key ID which is used along with <i>keychain-name</i> and direction to uniquely identify this particular key entry.</p> <p><i>authentication-key</i> — Specifies the <i>authentication-key</i> that will be used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.</p> <p>The <i>authentication-key</i> can be any combination of letters or numbers. .</p> <p>Values A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.</p> <p>algorithm-<i>algorithm</i> — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.</p> <p>Values aes-128-cmac-96 — Specifies an algorithm based on the AES standard hmac-sha-1-96 — Specifies an algorithm based on SHA-1.</p> <p><i>hash-key</i> / <i>hash2-key</i> — The hash key. The key can be any combination of ASCII characters up to 33 for the <i>hash-key</i> and 96 characters for the <i>hash2-key</i> in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).</p> <p>This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.</p> <p>hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.</p> <p>hash2 — Specifies the key is entered in a more complex encrypted form.</p>

begin-time

Syntax	begin-time [<i>date</i>] [<i>hours-minutes</i>] [UTC] [now] [forever]
Context	config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
Description	<p>This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.</p> <p>If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.</p>
Parameters	<p><i>date hours-minutes</i> — Specifies the date and time for the key to become active.</p> <p>Values date: YYYY/MM/DD hours-minutes: hh:mm[:ss]</p>

now — Specifies the the key should become active immediately.

forever — Specifies that the key should always be active.

end-time

Syntax	end-time [<i>date</i>] [<i>hours-minutes</i>] [UTC] [now] [forever]
Context	config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
Description	This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream.
Default	forever
Parameters	<p><i>date</i> — Specifies the calendar date after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the YYYY/MM/DD format. When no year is specified the system assumes the current year.</p> <p><i>hours-minutes</i> — Specifies the time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the hh:mm[:ss] format. Seconds are optional, and if not included, assumed to be 0.</p> <p>UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.</p> <p>now — Specifies a time equal to the current system time.</p> <p>forever — Specifies a time beyond the current epoch.</p>

tolerance

Syntax	tolerance [<i>seconds</i> forever]
Context	config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry
Description	This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.
Parameters	<p><i>seconds</i> — Specifies the duration that an eligible receive key overlaps with the active send key.</p> <p>Values 0 — 4294967294 seconds</p> <p>forever — Specifies that an eligible receive key overlap with the active send key forever.</p>

tcp-option-number

Syntax **tcp-option-number**

Configuration Commands

Context config>system>security>keychain

Description This command enables the context to configure the TCP option number to be placed in the TCP packet header.

receive

Syntax **receive** *option-number*

Context config>system>security>keychain>tcp-option-number

Description This command configures the TCP option number accepted in TCP packets received.

Default 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254, 253&254

send

Syntax **send** *option-number*

Context config>system>security>keychain>tcp-option-number

Description This command configures the TCP option number accepted in TCP packets sent.

Default 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254

dst-port

Syntax **dst-port** [**tcp/udp** *port-number*] [*mask*]
no dst-port

Context config>sys>sec>cpm>entry>match

Description This command specifies the TCP/UDP port to match the destination-port of the packet. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

The **no** form of the command removes the destination port match criterion.

Parameters *dst-port-number* — Specifies the destination port number to be used as a match criteria expressed as a decimal integer.

Values 0 — 65535 (accepted in decimal hex or binary)

mask — Specifies the 16 bit mask to be applied when matching the destination port.

Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

clear-lockout

Syntax {*user-name*} **clear-lockout**

Context admin>user

Description This command is used to clear any lockouts for a specific user.

Parameters *name* — Specifies locked user name.

Show Commands

Security Commands

access-group

Syntax	access-group [<i>group-name</i>]
Context	show>system>security
Description	This command displays SNMP access group information.
Parameters	<i>group-name</i> — This command displays information for the specified access group.
Output	Security Access Group Output — The following table describes security access group output fields..

Table 6: Show System Security Access Group Output Fields

Label	Description
Group name	The access group name.
Security model	The security model required to access the views configured in this node.
Security level	Specifies the required authentication and privacy levels to access the views configured in this node.
Read view	Specifies the variable of the view to read the MIB objects.
Write view	Specifies the variable of the view to configure the contents of the agent.
Notify view	Specifies the variable of the view to send a trap about MIB objects.

Sample Output

```
A:ALA-4# show system security access-group
=====
Access Groups
=====
group name      security  security  read      write      notify
                model     level     view      view       view
-----
snmp-ro        snmpv1   none      no-security          no-security
snmp-ro        snmpv2c  none      no-security          no-security
snmp-rw        snmpv1   none      no-security  no-security  no-security
snmp-rw        snmpv2c  none      no-security  no-security  no-security
snmp-rwa      snmpv1   none      iso          iso          iso
snmp-rwa      snmpv2c  none      iso          iso          iso
```

```
snmp-trap          snmpv1    none          iso
snmp-trap          snmpv2c  none          iso
=====
A:ALA-7#
```

authentication

- Syntax** **authentication [statistics]**
- Context** show>system>security
- Description** This command displays system login authentication configuration and statistics.
- Parameters** **statistics** — Appends login and accounting statistics to the display.
- Output** **Authentication Output** — The following table describes system security authentication output fields.

Table 7: Show System Security Authentication Output Fields

Label	Description
Sequence	The sequence in which authentication is processed.
Server address	The IP address of the RADIUS server.
Status	Current status of the RADIUS server.
Type	The authentication type.
Timeout (secs)	The number of seconds the router waits for a response from a RADIUS server.
Single connection	Enabled — Specifies a single connection to the TACACS+ server and validates everything via that connection. Disabled — The TACACS+ protocol operation is disabled.
Retry count	Displays the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.
Connection errors	Displays the number of times a user has attempted to login irrespective of whether the login succeeded or failed.
Accepted logins	The number of times the user has successfully logged in.
Rejected logins	The number of unsuccessful login attempts.
Sent packets	The number of packets sent.
Rejected packets	The number of packets rejected.

Sample Output

```

A:ALA-4# show system security authentication
=====
Authentication                sequence : radius tacplus local
=====
server address  status  type    timeout(secs)  single connection  retry count
-----
10.10.10.103   up      radius  5              n/a                 5
10.10.0.1      up      radius  5              n/a                 5
10.10.0.2      up      radius  5              n/a                 5
10.10.0.3      up      radius  5              n/a                 5
-----
radius admin status : down
tacplus admin status : up
health check       : enabled
-----
No. of Servers: 4
=====
A:ALA-4#

A:ALA-7>show>system>security# authentication statistics
=====
Authentication                sequence : radius tacplus local
=====
server address  status  type    timeout(secs)  single connection  retry count
-----
10.10.10.103   up      radius  5              n/a                 5
10.10.0.1      up      radius  5              n/a                 5
10.10.0.2      up      radius  5              n/a                 5
10.10.0.3      up      radius  5              n/a                 5
-----
radius admin status : down
tacplus admin status : up
health check       : enabled
-----
No. of Servers: 4
=====
Login Statistics
=====
server address  connection errors  accepted logins  rejected logins
-----
10.10.10.103   0                  0                0
10.10.0.1      0                  0                0
10.10.0.2      0                  0                0
10.10.0.3      0                  0                0
local          n/a                1                0
=====
Authorization Statistics (TACACS+)
=====
server address  connection errors  sent packets  rejected packets
-----
Accounting Statistics
=====
server address  connection errors  sent packets  rejected packets
-----
10.10.10.103   0                  0                0

```

Show Commands

```
10.10.0.1          0          0          0
10.10.0.2          0          0          0
10.10.0.3          0          0          0
=====
A:ALA-7#
```

communities

- Syntax** **communities**
- Context** show>system>security
- Description** This command displays SNMP communities.
- Output** **Communities Output** — The following table describes community output fields.

Table 8: Show Communities Output Fields

Label	Description
Community	The community string name for SNMPv1 and SNMPv2c access only.
Access	r — The community string allows read-only access. rw — The community string allows read-write access. rwa — The community string allows read-write access.
View	The view name.
Version	The SNMP version.
Group Name	The access group name.
No of Communities	The total number of configured community strings.

Sample Output

```
A:ALA-48# show system security communities
=====
Communities
=====
community      access  view          version  group name
-----
cli-readonly   r       iso           v2c     cli-readonly
cli-readwrite  rw      iso           v2c     cli-readwrite
public         r       no-security   v1 v2c  snmp-ro
-----
No. of Communities: 3
=====
A:ALA-48#
```

keychain

Syntax	keychain [<i>key-chain</i>] [detail]
Context	show>system>security
Description	This command displays keychain information.
Parameters	<i>key-chain</i> — Specifies the keychain name to display. detail — Displays detailed keychain information.

Sample Output

```
*A:ALA-A# show system security keychain test
=====
Key chain:test
=====
TCP-Option number send      : 254                Admin state   : Up
TCP-Option number receive   : 254                Oper state    : Up
=====
*A:ALA-A#

*A:ALA-A# show system security keychain test detail
=====
Key chain:test
=====
TCP-Option number send      : 254                Admin state   : Up
TCP-Option number receive   : 254                Oper state    : Up
=====
Key entries for key chain: test
=====
Id          : 0
Direction  : send-receive          Algorithm     : hmac-sha-1-96
Admin State : Up                          Valid        : Yes
Active     : Yes                     Tolerance    : 300
Begin Time  : 2007/02/15 18:28:37   Begin Time (UTC) : 2007/02/15 17:28:37
End Time    : N/A                    End Time (UTC)   : N/A
=====
Id          : 1
Direction  : send-receive          Algorithm     : aes-128-cmac-96
Admin State : Up                          Valid        : Yes
Active     : No                       Tolerance    : 300
Begin Time  : 2007/02/15 18:27:57   Begin Time (UTC) : 2007/02/15 17:27:57
End Time    : 2007/02/15 18:28:13   End Time (UTC)   : 2007/02/15 17:28:13
=====
Id          : 2
Direction  : send-receive          Algorithm     : aes-128-cmac-96
Admin State : Up                          Valid        : Yes
Active     : No                       Tolerance    : 500
Begin Time  : 2007/02/15 18:28:13   Begin Time (UTC) : 2007/02/15 17:28:13
End Time    : 2007/02/15 18:28:37   End Time (UTC)   : 2007/02/15 17:28:37
```

```
=====
*A:ALA-A#
```

management-access-filter

- Syntax** `management-access-filter`
- Context** `show>system>security`
- Description** This command displays management access filter information for IP and MAC filters.

ip-filter

- Syntax** `ip-filter [entry entry-id]`
- Context** `show>system>security>mgmt-access-filter`
- Description** This command displays management-access IP filters.
- Parameters** *entry-id* — Displays information for the specified entry.

Values 1 — 9999

Output Management Access Filter Output — The following table describes management access filter output fields.

Table 9: Show Management Access Filter Output Fields

Label	Description
Def. action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted. Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued. Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied.
Entry	The entry ID in a policy or filter table.
Description	A text string describing the filter.
Src IP	The source IP address used for management access filter match criteria.
Src Interface	The interface name for the next-hop to which the packet should be forwarded if it hits this filter entry.
Dest port	The destination port.

Table 9: Show Management Access Filter Output Fields (Continued)

Label	Description
Match	The number of times a management packet has matched this filter entry.
Protocol	The IP protocol to match.
Action	The action to take for packets that match this filter entry.
Flow label	The flow label value to match.
Next-header	The IPv6 next header value to match.
L4 Src port	The TCP/UDP source port number to match.
Fragment	Indicates if the entry should match a fragment or not.
Router	Router Instance ID to match.
Log	Indicates if packet matching this entry must be logged or not. On 7210 platforms logging is not supported.

```

Output *7210-SAS>show>system>security>management-access-filter# ip-filter entry 1

=====
IPv4 Management Access Filter
=====
filter type      : ip
Def. Action      : permit
Admin Status     : enabled (no shutdown)
-----
Entry            : 1
Description      : (Not Specified)
Src IP           : undefined
Src interface    : undefined
Dest port        : undefined
L4 Src port      : undefined
Fragment         : off
Protocol         : undefined
Router           : undefined
Action           : none
Log              : disabled
Matches          : 0
=====
*7210-SAS>show>system>security>management-access-filter#

```

ipv6-filter

- Syntax** `ipv6-filter [entry entry-id]`
- Context** `show>system>security>mgmt-access-filter`
- Description** This command displays management-access IPv6 filters.
- Parameters** *entry-id* — Displays information for the specified entry.

Values 1 — 9999

Output Management Access Filter Output — The following table describes management access filter output fields for IPv6 filters.

Table 10: Show Management Access Filter Output Fields

Label	Description
Def. action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted. Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued. Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied.
Entry	The entry ID in a policy or filter table.
Description	A text string describing the filter.
Src IP	The source IPv6 address used for management access filter match criteria.
Src Interface	The interface name for the next-hop to which the packet should be forwarded if it hits this filter entry.
Dest port	The destination port.
Flow label	The flow label value to match.
Protocol	The IPv6 protocol to match.
Action	The action to take for packets that match this filter entry.
Next-header	The IPv6 next header value to match.
L4 Src port	The TCP/UDP source port number to match.
Router	Router Instance ID to match.
Log	Indicates if packet matching this entry must be logged or not. On 7210 platforms logging is not supported.

```
A:7210SAS# show system security management-access-filter ipv6-filter

=====
IPv6 Management Access Filter
=====
filter type : ipv6
Def. Action : permit
Admin Status : enabled (no shutdown)
-----
Entry : 1
Description : (Not Specified)
Src IP : undefined
Flow label : undefined
Src interface : 1/1/1
Dest port : undefined
L4 Src port : undefined
Next-header : undefined
Router : undefined
Action : permit
Log : disabled
Matches : 0
=====
*A:7210SAS#
```

password-options

Syntax password-options

Context show>system>security

Description This command displays configured password options.

Output **Password Options Output** — The following table describes password options output fields.

Table 11: Show Management Access Filter Output Fields

Label	Description
Password aging in days	Displays the number of days a user password is valid before the user must change their password.
Number of invalid attempts permitted per login	Displays the number of unsuccessful login attempts allowed for the specified time .
Time in minutes per login attempt	Displays the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.
Lockout period (when threshold breached)	Displays the lockout period in minutes where the user is not allowed to login.
Authentication order	Displays the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords.

Table 11: Show Management Access Filter Output Fields (Continued)

Label	Description
Configured complexity options	Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the authentication section.
Minimum password length	Displays the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and DES-keys configured in the system security section.

Sample Output

```
A:ALA-7# show system security password-options
=====
Password Options
=====
Password aging in days                : none
Number of invalid attempts permitted per login : 3
Time in minutes per login attempt      : 5
Lockout period (when threshold breached) : 10
Authentication order                  : radius tacplus local
Configured complexity options         :
Minimum password length                : 6
=====
A:ALA-7#
```

profile

- Syntax** **profile** [*profile-name*]
- Context** show>system>security
- Description** This command displays user profile information.
If the *profile-name* is not specified, then information for all profiles are displayed.
- Parameters** **profile-name** — Displays information for the specified user profile.
- Output** **User Profile Output** — The following table describes user profile output fields.

Table 12: Show User Profile Output Fields

Label	Description
User Profile	Displays the profile name used to deny or permit user console access to a hierarchical branch or to specific commands.

Table 12: Show User Profile Output Fields (Continued)

Label	Description
Def. action	Permit all – Permits access to all commands. Deny – Denies access to all commands. None – No action is taken.
Entry	The entry ID in a policy or filter table.
Description	Displays the text string describing the entry.
Match Command	Displays the command or subtree commands in subordinate command levels.
Action	Permit all – Commands matching the entry command match criteria are permitted. Deny – Commands not matching the entry command match criteria are not permitted.
No. of profiles	The total number of profiles listed.

Sample Output

```
A:ALA-7# show system security profile administrative
=====
User Profile
=====
User Profile : administrative
Def. Action  : permit-all
-----
Entry       : 10
Description :
Match Command: configure system security
Action      : permit
-----
Entry       : 20
Description :
Match Command: show system security
Action      : permit
-----
No. of profiles:
=====
A:ALA-7#
```

source-address

- Syntax** `source-address`
- Context** `show>system>security`
- Description** This command displays source-address configured for applications.
- Output** **Source Address Output** — The following table describes source address output fields.

Table 13: Show Source Address Output Fields

Label	Description
Application	Displays the source-address application.
IP address Interface Name	Displays the source address IP address or interface name.
Oper status	Up — The source address is operationally up. Down — The source address is operationally down.

Sample Output

```
A:SR-7# show system security source-address
=====
Source-Address applications
=====
Application          IP address/Interface Name          Oper status
-----
telnet               10.20.1.7                          Up
radius              loopback1                          Up
=====
A:SR-7#
```

ssh

- Syntax** `ssh`
- Context** `show>system>security`
- Description** This command displays all the SSH sessions as well as the SSH status and fingerprint.
- Output** **SSH Options Output** — The following table describes SSH output fields .

Label	Description
SSH status	SSH is enabled — Displays that SSH server is enabled. SSH is disabled — Displays that SSH server is disabled.

Label	Description (Continued)
SSH Preserve Key	Enabled – Displays that preserve-key is enabled. Disabled – Displays that preserve-key is disabled.
SSH protocol version 1	Enabled – Displays that SSH1 is enabled. Disabled – Displays that SSH1 is disabled.
SSH protocol version 2	Enabled – Displays that SSH2 is enabled. Disabled – Displays that SSH2 is disabled.
Key fingerprint	The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected router(s) (remote client).
Encryption	des — Data encryption using a private (secret) key. 3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.
Username	The name of the user.
Number of SSH sessions	The total number of SSH sessions.

Sample output

NOTE: SSH is enabled by default for both IPv4 and IPv6 when the node boots up.

```
ALA-7# show system security ssh
SSH is enabled
SSH preserve key: Enabled
SSH protocol version 1: Enabled
RSA host key finger print:c6:a9:57:cb:ee:ec:df:33:1a:cd:d2:ef:3f:b5:46:34

SSH protocol version 2: Enabled
DSA host key finger print:ab:ed:43:6a:75:90:d3:fc:42:59:17:8a:80:10:41:79
=====
Connection      Encryption      Username
=====
192.168.5.218    3des           admin
-----
Number of SSH sessions : 1
=====
ALA-7#
A:ALA-49>config>system>security# show system security ssh
SSH is disabled
A:ALA-49>config>system>security#
```

user

- Syntax** **user** [*user-id*] [**detail**]
- Context** show>system>security
- Description** This command displays user registration information.
If no command line options are specified, summary information for all users displays.
- Parameters** *user-id* — Displays information for the specified user.
 - Default** All users
 - detail** — Displays detailed user information to the summary output.
- Output** **User Output** — The following table describes user output fields.

Label	Description
User ID	The name of a system user.
Need new pwd	Y — The user must change his password at the next login.
	N — The user is not forced to change his password at the next login.
Cannot change pw	Y — The user has the ability to change the login password.
	N — The user does not have the ability to change the login password.
User permissions	Console — Y - The user is authorized for console access. N- The user is not authorized for console access.
	FTP — Y - The user is authorized for FTP access. N - The user is not authorized for FTP access.
	SNMP — Y - The user is authorized for SNMP access. N - The user is not authorized for SNMP access.
Password expires	The number of days in which the user must change his login password.
Attempted logins	The number of times the user has attempted to login irrespective of whether the login succeeded or failed.
Failed logins	The number of unsuccessful login attempts.
Local conf	Y — Password authentication is based on the local password database.
	N — Password authentication is not based on the local password database.
Home directory	Specifies the local home directory for the user for both console and FTP access.

Label	Description (Continued)
Restricted to home	<p>Yes – The user is not allowed to navigate to a directory higher in the directory tree on the home directory device.</p> <p>No – The user is allowed to navigate to a directory higher in the directory tree on the home directory device.</p>
Login exec file	Displays the user's login exec file which executes whenever the user successfully logs in to a console session.

Sample Output

```
A:ALA-7# show system security user
=====
Users
=====
user id          need   user permissions password  attempted failed  local
                new pwd console ftp snmp  expires  logins  logins  conf
-----
admin            n     y      n  n    never    21     0     y
=====
A:ALA-7#

A:
ALA-7# show system security user detail
=====
Users
=====
user id          need   user permissions password  attempted failed  local
                new pwd console ftp snmp  expires  logins  logins  conf
-----
admin            n     y      n  n    never    21     0     y
=====

=====
User Configuration Detail
=====
user id          : admin
-----
console parameters
-----
new pw required  : no                cannot change pw  : no
home directory   : cf1:\
restricted to home : no
login exec file  :
profile          : administrative
-----
snmp parameters
=====
A:ALA-7#
```

view

- Syntax** `view [view-name] [detail]`
- Context** `show>system>security`
- Description** This command displays the SNMP MIB views.
- Parameters**
 - view-name* — Specify the name of the view to display output. If no view name is specified, the complete list of views displays.
 - detail** — Displays detailed view information.
- Output** **View Output** — The following table describes show view output fields.

Table 14: Show View Output Fields

Label	Description
view name	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.
oid tree	The object identifier of the ASN.1 subtree.
mask	The bit mask that defines a family of view subtrees.
permission	Indicates whether each view is included or excluded
No. of Views	Displays the total number of views.

Sample Output

```
A:ALA-48# show system security view
=====
Views
=====
view name      oid tree      mask          permission
-----
iso            1             11111111     included
read1         1.1.1.1      11111111     included
writel        2.2.2.2      11111111     included
testview      1             11111111     included
testview      1.3.6.1.2    11111111     excluded
mgmt-view     1.3.6.1.2.1.2  included
mgmt-view     1.3.6.1.2.1.4  included
mgmt-view     1.3.6.1.2.1.5  included
mgmt-view     1.3.6.1.2.1.6  included
mgmt-view     1.3.6.1.2.1.7  included
mgmt-view     1.3.6.1.2.1.31 included
mgmt-view     1.3.6.1.2.1.77 included
mgmt-view     1.3.6.1.4.1.6527.3.1.2.3.7 included
mgmt-view     1.3.6.1.4.1.6527.3.1.2.3.11 included
no-security   1             included
no-security   1.3.6.1.6.3   excluded
```

```

no-security      1.3.6.1.6.3.10.2.1      included
no-security      1.3.6.1.6.3.11.2.1      included
no-security      1.3.6.1.6.3.15.1.1      included
on-security      2                      00000000      included
-----
No. of Views:
=====
A:ALA-48#

```

static-sa

Syntax **static-sa**
static-sa name sa-name
static-sa spi spi

Context show>ipsec

Description This command displays IPsec static-SA information.

Parameters *sa-name* — Specifies the SA name.
 Values 32 chars max

spi — Specifies the spi.
 Values 256..16383

Login Control

users

- Syntax** **users**
- Context** show
- Description** Displays console user login and connection information.
- Output** **Users Output** — The following table describes show users output fields.

Table 15: Show Users Output Fields

Label	Description
User	The user name.
Type	The user is authorized this access type.
From	The originating IP address.
Login time	The time the user logged in.
Idle time	The amount of idle time for a specific login.
Number of users	Displays the total number of users logged in.

Sample Console Users Output

```
A:ALA-7# show users
=====
User           Type    From      Login time      Idle time
=====
testuser       Console --         21FEB2007 04:58:55 0d 00:00:00 A
=====
Number of users : 1
'A' indicates user is in admin mode
=====
A:ALA-7#
```

Debug Commands

radius

Syntax	radius [detail] [hex] no radius
Context	debug
Description	This command enables debugging for RADIUS connections. The no form of the command disables the debugging.
Parameters	detail — Displays detailed output. hex — Displays the packet dump in hex format.

Show Commands

In This Chapter

This chapter provides information to configure SNMP.

Topics in this chapter include:

- [SNMP Overview on page 162](#)
 - [SNMP Architecture on page 162](#)
 - [Management Information Base on page 162](#)
 - [SNMP Protocol Operations on page 163](#)
 - [SNMP Versions on page 163](#)
 - [Management Information Access Control on page 164](#)
 - [User-Based Security Model Community Strings on page 165](#)
 - [Views on page 165](#)
 - [Access Groups on page 165](#)
 - [Users on page 166](#)
- [Which SNMP Version to Use? on page 167](#)
- [Configuration Notes on page 169](#)

SNMP Overview

SNMP Architecture

The Service Assurance Manager (SAM) is comprised of two elements: managers and agents. The manager is the entity through which network management tasks are facilitated. Agents interface managed objects. Managed devices, such as bridges, hubs, routers, and network servers can contain managed objects. A managed object can be a configuration attribute, performance statistic, or control action that is directly related to the operation of a device.

Managed devices collect and store management information and use Simple Network Management Protocol (SNMP). SNMP is an application-layer protocol that provides a message format to facilitate communication between SNMP managers and agents. SNMP provides a standard framework to monitor and manage devices in a network from a central location.

An SNMP manager controls and monitors the activities of network hosts which use SNMP. An SNMP manager can obtain (get) a value from an SNMP agent or store (set) a value in the agent. The manager uses definitions in the management information base (MIB) to perform operations on the managed device such as retrieving values from variables or blocks of data, replying to requests, and processing traps.

Between the SNMP agent and the SNMP manager the following actions can occur:

- The manager can get information from the agent.
- The manager can set the value of a MIB object that is controlled by an agent.
- The agent can send traps to notify the manager of significant events that occur on the router.

Management Information Base

A MIB is a formal specifications document with definitions of management information used to remotely monitor, configure, and control a managed device or network system. The agent's management information consists of a set of network objects that can be managed with SNMP. Object identifiers are unique object names that are organized in a hierarchical tree structure. The main branches are defined by the Internet Engineering Task Force (IETF). When requested, the Internet Assigned Numbers Authority (IANA) assigns a unique branch for use by a private organization or company. The branch assigned to Alcatel-Lucent (TiMetra) is 1.3.6.1.4.1.6527.

The SNMP agent provides management information to support a collection of IETF specified MIBs and a number of MIBs defined to manage device parameters and network data unique to Alcatel-Lucent's router.

SNMP Protocol Operations

Between the SNMP agent and the SNMP manager the following actions can occur:

- The manager can get information from the agent.
 - The manager can set the value of a MIB object that is controlled by an agent.
 - The agent notifies the manager of significant events that occur on the router.
-

SNMP Versions

The agent supports multiple versions of the SNMP protocol.

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.
SNMPv1 uses a community string match for authentication.
- The implementation uses SNMPv2c, the community-based administrative framework for SNMPv2. SNMPv2c uses a community string match for authentication.
- In SNMP Version 3 (SNMPv3), USM defines the user authentication and encryption features. View Access Control MIB (VACM) defines the user access control features. The SNMP-COMMUNITY-MIB is used to associate SNMPv1/SNMPv2c community strings with SNMPv3 VACM access control.
SNMPv3 uses a username match for authentication.

Management Information Access Control

By default, the implementation of SNMP uses SNMPv3. SNMPv3 incorporates security model and security level features. A security model is the authentication type for the group and the security level is the permitted level of security within a security model. The combination of the security level and security model determines which security mechanism handles an SNMP packet.

To implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. These access groups provide standard read-only, read-write, and read-write-all access groups and views that can simply be assigned community strings. In order to implement SNMP with security features, security models, security levels, and USM communities must be explicitly configured. Optionally, additional views which specify more specific OIDs (MIB objects in the subtree) can be configured.

Access to the management information in an SNMPv1/SNMPv2c agent is controlled by the inclusion of a community name string in the SNMP request. The community defines the subset of the agent's managed objects that can be accessed by the requester. It also defines what type of access is allowed: read-only or read-write.

The use of community strings provides minimal security and context checking for both agents and managers that receive requests and initiate trap operations. A community string is a text string that acts like a password to permit access to the agent on the router.

Alcatel-Lucent's implementation of SNMP has defined three levels of community-named access:

- Read-Only permission — Grants only read access to objects in the MIB, except security objects.
- Read-Write permission — Grants read and write access to all objects in the MIB, except security objects.
- Read-Write-All permission — Grants read and write access to all objects in the MIB, including security objects.

User-Based Security Model Community Strings

User-based security model (USM) community strings associates a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

Views

Views control the access to a managed object. The total MIB of a router can be viewed as a hierarchical tree. When a view is created, either the entire tree or a portion of the tree can be specified and made available to a user to manage the objects contained in the subtree. Object identifiers (OIDs) uniquely identify managed objects. A view defines the type of operations for the view such as read, write, or notify.

OIDs are organized in a hierarchical tree with specific values assigned to different organizations. A view defines a subset of the agent's managed objects controlled by the access rules associated with that view.

Pre-defined views are available that are particularly useful when configuring SNMPv1 and SNMPv2c.

The Alcatel-Lucent SNMP agent associates SNMPv1 and SNMPv2c community strings with a SNMPv3 view.

Access Groups

Access groups associate a user group and a security model to the views the group can access. An access group is defined by a unique combination of a group name, security model (SNMPv1, SNMPv2c, or SNMPv3), and security level (no-authorization-no-privacy, authorization-no-privacy, or privacy).

An access group, in essence, is a template which defines a combination of access privileges and views. A group can be associated to one or more network users to control their access privileges and views.

Additional access parameters must be explicitly configured if the preconfigured access groups and views for SNMPv1 and SNMPv2c do not meet your security requirements.

Users

By default, authentication and encryption parameters are not configured. Authentication parameters which a user must use in order to be validated by the device can be modified. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with.

User access and authentication privileges must be explicitly configured. In a user configuration, a user is associated with an access group, which is a collection of users who have common access privileges and views (see [Access Groups](#)).

Which SNMP Version to Use?

SNMPv1 and SNMPv2c do not provide security, authentication, or encryption. Without authentication, a non authorized user could perform SNMP network management functions and eavesdrop on management information as it passes from system to system. Many SNMPv1 and SNMPv2c implementations are restricted read-only access, which, in turn, reduces the effectiveness of a network monitor in which network control applications cannot be supported.

To implement SNMPv3, an authentication and encryption method must be assigned to a user in order to be validated by the device. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

[Figure 3](#) depicts the configuration requirements to implement SNMPv1/SNMPv2c, and SNMPv3.

Which SNMP Version to Use?

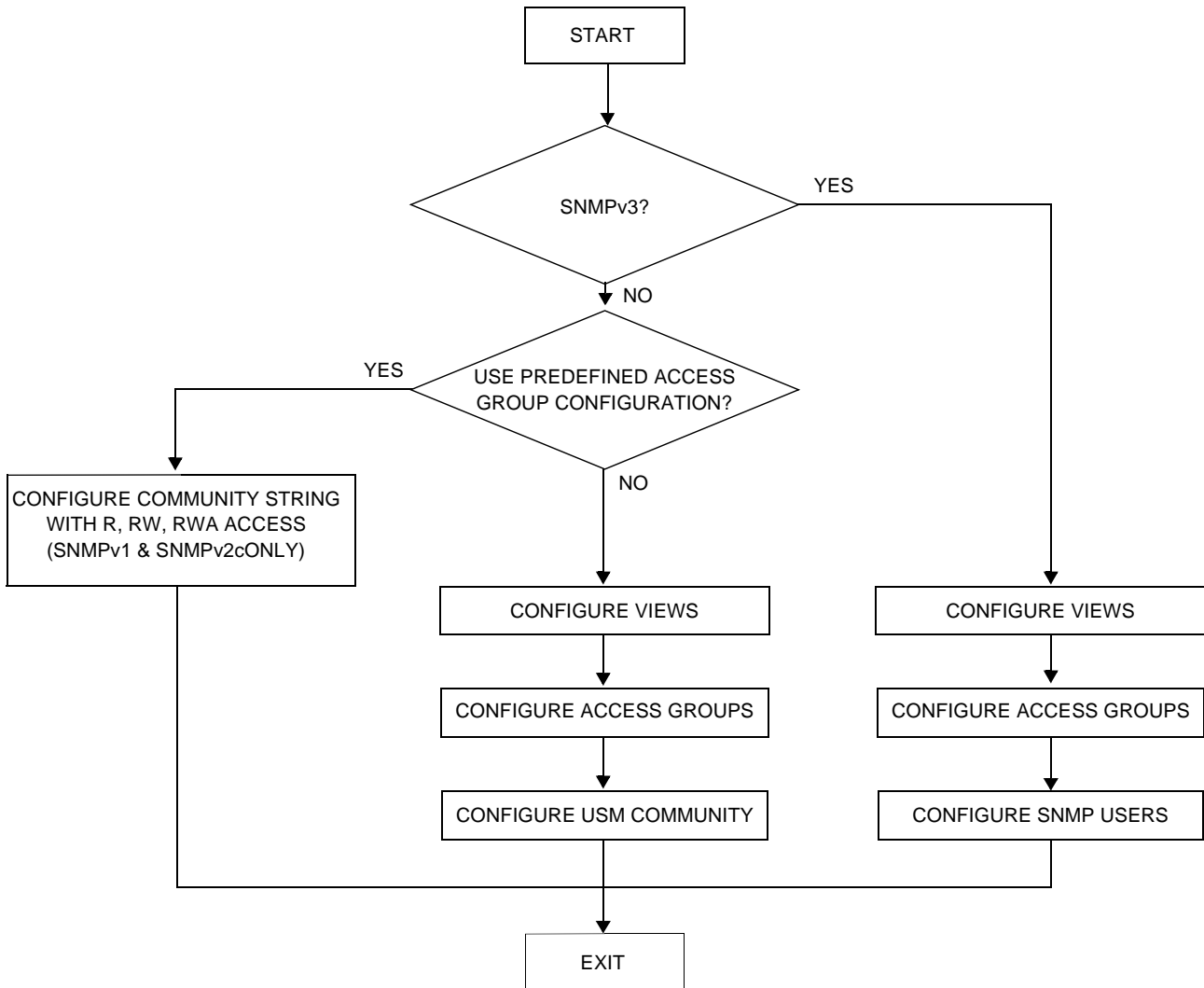


Figure 3: SNMPv1 and SNMPv2c Configuration and Implementation Flow

Configuration Notes

This section describes SNMP configuration caveats.

General

- To avoid management systems attempting to manage a partially booted system, SNMP will remain in a shut down state if the configuration file fails to complete during system startup. While shutdown, SNMP gets and sets are not processed. However, notifications are issued if an SNMP trap group has been configured.

In order to enable SNMP, the portions of the configuration that failed to load must be initialized properly. Start SNMP with the **config>system>snmp>no shutdown** CLI command.

- Use caution when changing the SNMP engine ID. If the SNMP engine ID is changed in the **config>system>snmp> engineID engine-id** context, the current configuration must be saved and a reboot must be executed. If not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.
- SNMP dying gasp uses system IP to send out packet. Therefore, the system IP must be configured before configuring SNMP dying gasp.

Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

- [SNMP Configuration Overview on page 172](#)
- [Basic SNMP Security Configuration on page 173](#)
- [Configuring SNMP Components on page 174](#)

SNMP Configuration Overview

This section describes how to configure SNMP components which apply to SNMPv1 and SNMPv2c, and SNMPv3 on the router.

- [Configuring SNMPv1 and SNMPv2c on page 172](#)
 - [Configuring SNMPv3 on page 172](#)
-

Configuring SNMPv1 and SNMPv2c

Alcatel-Lucent routers are based on SNMPv3. To use the routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three pre-defined access methods are available when SNMPv1 or SNMPv2c access is required. Each access method (**r**, **rw**, or **rwa**) is associated with an SNMPv3 access group that determines the access privileges and the scope of managed objects available. The **community** command is used to associate a community string with a specific access method and the required SNMP version (SNMPv1 or SNMPv2c). The access methods are:

- Read-Only — Grants read only access to the entire management structure with the exception of the security area.
- Read-Write — Grants read and write access to the entire management structure with the exception of the security area.
- Read-Write-All — Grants read and write access to the entire management structure, including security.

If the predefined access groups do not meet your access requirements, then additional access groups and views can be configured. The **usm-community** command is used to associate an access group with an SNMPv1 or SNMPv2c community string.

SNMP trap destinations are configured in the **config>log>snmp-trap-group** context.

Configuring SNMPv3

implements SNMPv3. If security features other than the default views are required, then the following parameters must be configured:

- Configure views
- Configure access groups
- Configure SNMP users

Basic SNMP Security Configuration

This section provides information to configure SNMP parameters and provides examples of common configuration tasks. The minimal SNMP parameters are:

For SNMPv1 and SNMPv2c:

- Configure community string parameters.

For SNMPv3:

- Configure view parameters
- Configure SNMP group
- Configure access parameters
- Configure user with SNMP parameters

The following displays SNMP default views, access groups, and attempts parameters.

```
A:ALA-1>config>system>security>snmp# info detail
-----
      view iso subtree 1
            mask ff type included
      exit
      view no-security subtree 1
            mask ff type included
      exit
      view no-security subtree 1.3.6.1.6.3
            mask ff type excluded
      exit
      view no-security subtree 1.3.6.1.6.3.10.2.1
            mask ff type included
      exit
      view no-security subtree 1.3.6.1.6.3.11.2.1
            mask ff type included
      exit
      view no-security subtree 1.3.6.1.6.3.15.1.1
            mask ff type included
      exit
      access group snmp-ro security-model snmpv1 security-level no-auth-no-pri-
vacancy read no-security notify no-security
            access group snmp-ro security-model snmpv2c security-level no-auth-no-pri-
vacancy read no-security notify no-security
            access group snmp-rw security-model snmpv1 security-level no-auth-no-pri-
vacancy read no-security write no-security notify no-security
            access group snmp-rw security-model snmpv2c security-level no-auth-no-pri-
vacancy read no-security write no-security notify no-security
            access group snmp-rwa security-model snmpv1 security-level no-auth-no-pri-
vacancy read iso write iso notify iso
            access group snmp-rwa security-model snmpv2c security-level no-auth-no-pri-
vacancy read iso write iso notify iso
            access group snmp-trap security-model snmpv1 security-level no-auth-no-pri-
vacancy notify iso
            access group snmp-trap security-model snmpv2c security-level no-auth-no-
privacy notify iso
      attempts 20 time 5 logout 10
```

Configuring SNMP Components

Use the CLI syntax displayed below to configure the following SNMP scenarios:

- [Configuring a Community String on page 175](#)
- [Configuring View Options on page 176](#)
- [Configuring Access Options on page 177](#)
- [Configuring USM Community Options on page 179](#)
- [Configuring Other SNMP Parameters on page 180](#)

CLI Syntax: `config>system>security>snmp`
`attempts [count] [time minutes1] [lockout minutes2]`
`community community-string access-permissions [version SNMP`
`version]`
`usm-community community-string group group-name`
`view view-name subtree oid-value`
`mask mask-value [type {included|excluded}]`
`access group group-name security-model security-model secu-`
`rity-level security-level [context context-name [pre-`
`fix-match]] [read view-name-1] [write view-name-2]`
`[notify view-name-3]`

Configuring a Community String

SNMPv1 and SNMPv2c community strings are used to define the relationship between an SNMP manager and agent. The community string acts like a password to permit access to the agent. The access granted with a community string is restricted to the scope of the configured group.

One or more of these characteristics associated with the string can be specified:

- Read-only, read-write, and read-write-all permission for the MIB objects accessible to the community.
- The SNMP version, SNMPv1 or SNMPv2c.

Default access features are pre-configured by the agent for SNMPv1/SNMPv2c.

Use the following CLI syntax to configure community options:

CLI Syntax: `config>system>security>snmp
community community-string access-permissions [version SNMP
version]`

The following displays an SNMP community configuration example:

```
*A:cses-A13>config>system>security>snmp# info
-----
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both
-----
*A:cses-A13>config>system>security>snmp#
```

Configuring View Options

Use the following CLI syntax to configure view options:

CLI Syntax: `config>system>security>snmp`
`view view-name subtree oid-value`
`mask mask-value [type {included|excluded}]`

The following displays a view configuration example:

```
*A:cses-A13>config>system>security>snmp# info
-----
view "testview" subtree "1"
mask ff
exit
view "testview" subtree "1.3.6.1.2"
mask ff type excluded
exit
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both
-----
*A:cses-A13>config>system>security>snmp#
```

Configuring Access Options

The **access** command creates an association between a user group, a security model and the views that the user group can access. Access must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Use the following CLI syntax to configure access features:

CLI Syntax: `config>system>security>snmp`
`access group group-name security-model security-model security-level security-level [context context-name [prefix-match]] [read view-name-1] [write view-name-2] [notify view-name-3]`

The following displays an access configuration with the view configurations.

```
*A:cses-A13>config>system>security>snmp# info
-----
view "testview" subtree "1"
  mask ff
  exit
view "testview" subtree "1.3.6.1.2"
  mask ff type excluded
  exit
access group "test" security-model usm security-level auth-no-privacy read "testview" write "testview" notify "testview"
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both
-----
*A:cses-A13>config>system>security>snmp#
```

Configuring SNMP Components

Use the following CLI syntax to configure user group and authentication parameters:

CLI Syntax: config>system>security# user user-name
access [ftp] [snmp] [console]
snmp
authentication [none]|[[hash]{md5 key|sha key } privacy
{none|des-key key}]
group group-name

The following displays a user's SNMP configuration example.

```
A:ALA-1>config>system>security# info
-----
user "testuser"
  access snmp
  snmp
  authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
  group testgroup
  exit
exit
...
-----
A:ALA-1>config>system>security#
```

Configuring USM Community Options

User-based security model (USM) community strings associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

By default, the implementation of SNMP uses SNMPv3. However, to implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

CLI Syntax: `config>system>security>snmp`
`usm-community community-string group group-name`

The following displays a SNMP community configuration example:

```
A:ALA-1>config>system>security>snmp# info
-----
view "testview" subtree "1"
    mask ff
    exit
    view "testview" subtree "1.3.6.1.2"
        mask ff type excluded
    exit
    access group "test" security-model usm security-level auth-no-pr
ivacy read "testview" write "testview" notify "testview"
    community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
    community "Lla.RtAyRW2" hash2 r version v2c
    community "r0a159kIOfg" hash2 r version both
-----
A:ALA-1>config>system>security>snmp#
```

The group **grouptest** was configured in the `config>system>security>snmp>access` CLI context.

Configuring Other SNMP Parameters

Use the following CLI syntax to modify the system SNMP options:

CLI Syntax: `config>system>snmp`
`engineID engine-id`
`general-port port`
`packet-size bytes`
`no shutdown`

The following example displays the system SNMP default values:

```
A:ALA-104>config>system>snmp# info detail
-----
      shutdown
      engineID "0000xxxx000000000xxxxx00"
      packet-size 1500
      general-port 161
-----
A:ALA-104>config>system>snmp#
```

SNMP Command Reference

Command Hierarchies

Configuration Commands

SNMP System Commands

```

config
  — system
    — snmp
      — engineID engine-id
      — no engineID
      — general-port port
      — no general-port
      — packet-size bytes
      — no packet-size
      — [no] shutdown

```

SNMP Security Commands

```

config
  — system
    — security
      — snmp
        — access group-name security-model security-model security-level security-level [context context-name [prefix-match]] [read view-name-1] [write view-name-2] [notify view-name-3]
        — no access group-name [security-model security-model] [security-level security-level] [context context-name [prefix-match]] [read view-name-1] [write view-name-2] [notify view-name-3]
        — attempts [count] [time minutes1] [lockout minutes2]
        — no attempts
        — community community-string [hash | hash2] access-permissions [version SNMP-version]
        — no community community-string [hash | hash2]
        — usm-community community-string [hash | hash2] group group-name
        — no usm-community community-string [hash | hash2]
        — view view-name subtree oid-value
        — no view view-name [subtree oid-value]
          — mask mask-value [type {included | excluded}]
          — no mask

```

SNMP Command Reference

The following commands configure user-specific SNMP features. Refer to the **Security** section for CLI syntax and command descriptions.

```
config
  — system
    — security
      — [no] users user-name
        — [no] snmp
          — authentication {[none] | [[hash] {md5 key-1 | sha key-1}
            privacy {privacy-level key-2}]
          — group group-name
          — [no] group
```

Show Commands

```
show
  — snmp
    — counters
  — system
    — information
    — security
      — access-group [group-name]
      — authentication [statistics]
      — communities
      — keychain [key-chain] [detail]
      — management-access-filter
        — ip-filter [entry entry-id]
      — password-options
      — profile [profile-name]
      — ssh
      — user [user-id] [detail]
      — view [view-name] [detail]
```

Configuration Commands

SNMP System Commands

engineID

Syntax	[no] engineID <i>engine-id</i>
Context	config>system>snmp
Description	<p>This command sets the SNMP engineID to uniquely identify the SNMPv3 node. By default, the engineID is generated using information from the system backplane.</p> <p>If SNMP engine ID is changed in the config>system>snmp> engineID <i>engine-id</i> context, the current configuration must be saved and a reboot must be executed. If not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.</p> <p>Note: In conformance with IETF standard RFC 2274, <i>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</i>, hashing algorithms which generate SNMPv3 MD5 or SHA security digest keys use the engineID. Changing the SNMP engineID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable.</p> <p>When a chassis is replaced, use the engine ID of the first system and configure it in the new system to preserve SNMPv3 security keys. This allows management stations to use their existing authentication keys for the new system.</p> <p>Ensure that the engine IDs are not used on multiple systems. A management domain can only have one instance of each engineID.</p> <p>The no form of the command reverts to the default setting.</p>
Default	The engine ID is system generated.
Parameters	<i>engine-id</i> — An identifier from 10 to 64 hexadecimal digits (5 to 32 octet number), uniquely identifying this SNMPv3 node. This string is used to access this node from a remote host with SNMPv3.

general-port

Syntax	general-port <i>port-number</i> no general-port
Context	config>system>snmp
Description	This command configures the port number used by this node to receive SNMP request messages and to send replies. Note that SNMP notifications generated by the agent are sent from the port specified in the config>log>snmp-trap-group>trap-target CLI command.

Configuration Commands

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

Default 161

Parameters *port-number* — The port number used to send SNMP traffic other than traps.

Values 1 — 65535 (decimal)

packet-size

Syntax **packet-size** *bytes*
no packet-size

Context config>system>snmp

Description This command configures the maximum SNMP packet size generated by this node. If the packet size exceeds the MTU size of the egress interface the packet will be fragmented.

The **no** form of this command to revert to default.

Default 1500 bytes

Parameters *bytes* — The SNMP packet size in bytes.

Values 484 — 9216

snmp

Syntax **snmp**

Context config>system

Description This command creates the context to configure SNMP parameters.

shutdown

Syntax [**no**] **shutdown**

Context config>system>snmp

Description This command administratively disables SNMP agent operations. System management can then only be performed using the command line interface (CLI). Shutting down SNMP does not remove or change configuration parameters other than the administrative state. This command does not prevent the agent from sending SNMP notifications to any configured SNMP trap destinations. SNMP trap destinations are configured under the **config>log>snmp-trap-group** context.

This command is automatically invoked in the event of a reboot when the processing of the configuration file fails to complete or when an SNMP persistent index file fails while the **bof persist on** command is enabled.

The **no** form of the command administratively enables SNMP which is the default state.

Default **no shutdown**

SNMP Security Commands

access

Syntax	[no] access group <i>group-name</i> security-model <i>security-model</i> security-level <i>security-level</i> [context <i>context-name</i> [prefix-match]] [read <i>view-name-1</i>] [write <i>view-name-2</i>] [notify <i>view-name-3</i>]
Context	config>system>security>snmp
Description	<p>This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.</p> <p>Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the community on page 188).</p> <p>Default access group configurations cannot be modified or deleted.</p> <p>To remove the user group with associated, security model(s), and security level(s), use: no access group <i>group-name</i></p> <p>To remove a security model and security level combination from a group, use: no access group <i>group-name</i> security-model {snmpv1 snmpv2c usm} security-level {no-auth-no-privacy auth-no-privacy privacy}</p>
Default	none
Parameters	<p><i>group-name</i> — Specify a unique group name up to 32 characters.</p> <p>security-model {snmpv1 snmpv2c usm} — Specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.</p> <p>security-level {no-auth-no-priv auth-no-priv privacy} — Specifies the required authentication and privacy levels to access the views configured in this node.</p> <p>security-level no-auth-no-privacy — Specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the none option.</p> <p>security-level auth-no-privacy — Specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the group and the user must be configured for authentication.</p> <p>security-level privacy — Specifies that both authentication and privacy (encryption) is required. When this option is configured, both the group and the user must be configured for authentication. The user must also be configured for privacy.</p> <p>context <i>context-name</i> — Specifies a set of SNMP objects that are associated with the context-name.</p>

The *context-name* is treated as either a full context-name string or a context name prefix depending on the keyword specified (**exact** or **prefix**).

read *view-name* — Specifies the keyword and variable of the view to read the MIB objects. This command must be configured for each view to which the group has read access.

Default none

write *view-name* — Specifies the keyword and variable of the view to configure the contents of the agent. This command must be configured for each view to which the group has write access.

Values Up to 32 characters

notify *view-name* — specifies keyword and variable of the view to send a trap about MIB objects. This command must be configured for each view to which the group has notify access.

Values none

attempts

Syntax	attempts [<i>count</i>] [time <i>minutes1</i>] [lockout <i>minutes2</i>] no attempts
Context	config>system>security>snmp
Description	<p>This command configures a threshold value of unsuccessful SNMP connection attempts allowed in a specified time frame. The command parameters are used to counter denial of service (DOS) attacks through SNMP.</p> <p>If the threshold is exceeded, the host is locked out for the lockout time period.</p> <p>If multiple attempts commands are entered, each command overwrites the previously entered command.</p> <p>The no form of the command resets the parameters to the default values.</p>
Default	attempts 20 time 5 lockout 10 — 20 failed SNMP attempts allowed in a 5 minute period with a 10 minute lockout for the host if exceeded.
Parameters	<p><i>count</i> — The number unsuccessful SNMP attempts allowed for the specified time.</p> <p>Default 20</p> <p>Values 1 — 64</p> <p>time <i>minutes1</i> — The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out.</p> <p>Default 5</p> <p>Values 0 — 60</p>

lockout *minutes2* — The lockout period in minutes where the host is not allowed to login. When the host exceeds the attempted count times in the specified time, then that host is locked out from any further login attempts for the configured time period.

Default 10

Values 0 — 1440

community

Syntax **community** *community-string* [**hash** | **hash2**] *access-permissions* [**version** *SNMP-version*]
no community *community-string*

Context config>system>security>snmp

Description This command creates SNMP community strings for SNMPv1 and SNMPv2c access. This command is used in combination with the predefined access groups and views. To create custom access groups and views and associate them with SNMPv1 or SNMPv2c access use the `usm-community` command.

When configured, `community` implies a security model for SNMPv1 and SNMPv2c only. For SNMPv3 security, the `access` command on page 186 must be configured.

The `no` form of the command removes a community string.

Default none

Parameters *community-string* — Configure the SNMPv1 / SNMPv2c community string.

Values hash, hash2

access-permissions — **r** — Grants only read access to objects in the MIB, except security objects.

- **rw** — Grants read and write access to all objects in the MIB, except security.
- **rwa** — Grants read and write access to all objects in the MIB, including security.
- **vppls-mgmt** — Assigns a unique SNMP community string to the management virtual router.

version {**v1** | **v2c** | **both**} — Configures the scope of the community string to be for SNMPv1, SNMPv2c, or both SNMPv1 and SNMPv2c access.

Default both

mask

Syntax **mask** *mask-value* [**type** {**included** | **excluded**}]
no mask

Context config>system>security>snmp>view *view-name*

Description The mask value and the mask type, along with the *oid-value* configured in the `view` command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.

Each bit in the mask corresponds to a sub-identifier position. For example, the most significant bit for the first sub-identifier, the next most significant bit for the second sub-identifier, and so on. If the bit position on the sub-identifier is available, it can be included or excluded.

For example, the MIB subtree that represents MIB-II is 1.3.6.1.2.1. The mask that catches all MIB-II would be 0xfc or 0b11111100.

Only a single mask may be configured per view and OID value combination. If more than one entry is configured, each subsequent entry overwrites the previous entry.

Per RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, each MIB view is defined by two sets of view subtrees, the included view subtrees, and the excluded view subtrees. Every such view subtree, both the included and the excluded ones, are defined in this table. To determine if a particular object instance is in a particular MIB view, compare the object instance's object identifier (OID) with each of the MIB view's active entries in this table. If none match, then the object instance is not in the MIB view. If one or more match, then the object instance is included in, or excluded from, the MIB view according to the value of `vacmViewTreeFamilyType` in the entry whose value of `vacmViewTreeFamilySubtree` has the most sub-identifiers.

The **no** form of this command removes the mask from the configuration.

Default	none
Parameters	<p><i>mask-value</i> — The mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view. (Default: all 1^s)</p> <p>The mask can be entered either:</p> <ul style="list-style-type: none"> • In hex. For example, 0xfc. • In binary. For example, 0b11111100. <p>Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.</p> <p>type {included excluded} — Specifies whether to include or exclude MIB subtree objects. <i>included</i> - All MIB subtree objects that are identified with a 1 in the mask are available in the view. (Default: <i>included</i>).</p> <p><i>excluded</i> - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view. (Default: <i>included</i>).</p> <p>Default included</p>

snmp

Syntax	snmp
Context	config>system>security
Description	This command creates the context to configure SNMPv1, SNMPv2, and SNMPv3 parameters.

usm-community

Syntax	usm-community <i>community-string</i> [hash hash2] group <i>group-name</i> no usm-community <i>community-string</i> [hash hash2]
Context	config>system>security>snmp
Description	<p>This command is used to associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.</p> <p>Alcatel-Lucent's SR OS implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (Version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views which specify more specific OIDs (MIB objects in the subtree) can be configured.</p> <p>The no form of this command removes a community string.</p>
Default	none
Parameters	<p><i>community-string</i> — Configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used.</p> <p>Values hash, hash2</p> <p><i>group</i> — Specify the group that governs the access rights of this community string. This group must be configured first in the config system security snmp access group context. (Default: none)</p>

view

Syntax	view <i>view-name</i> subtree <i>oid-value</i> no view <i>view-name</i> [subtree <i>oid-value</i>]
Context	config>system>security>snmp
Description	<p>This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.</p> <p>Once the subtree (OID) is identified, a mask can be created to select the portions of the subtree to be included or excluded for access using this particular view. See the mask command. The view(s) configured with this command can subsequently be used in read, write, and notify commands which are used to assign specific access group permissions to created views and assigned to particular access groups.</p> <p>Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.</p> <p>The no view <i>view-name</i> command removes a view and all subtrees.</p> <p>The no view <i>view-name</i> subtree <i>oid-value</i> removes a sub-tree from the view name.</p>
Default	No views are defined.

Parameters *view-name* — Enter a 1 to 32 character view name. (Default: *none*)

oid-value — The object identifier (OID) value for the *view-name*. This value, for example, 1.3.6.1.6.3.11.2.1, combined with the mask and include and exclude statements, configures the access available in the view.

It is possible to have a view with different subtrees with their own masks and include and exclude statements. This allows for customizing visibility and write capabilities to specific user requirements.

Show Commands

counters

- Syntax** `counters`
- Context** `show>snmp`
- Description** This command displays SNMP counters information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.
- Output** **Counters Output** — The following table describes SNMP counters output fields.

Table 16: Counters Output Fields

Label	Description
<code>in packets</code>	Displays the total number of messages delivered to SNMP from the transport service.
<code>in gets</code>	Displays the number of SNMP get request PDUs accepted and processed by SNMP.
<code>in getnexts</code>	Displays the number of SNMP get next PDUs accepted and processed by SNMP.
<code>in sets</code>	Displays the number of SNMP set request PDUs accepted and processed by SNMP.
<code>out packets</code>	Displays the total number of SNMP messages passed from SNMP to the transport service.
<code>out get responses</code>	Displays the number of SNMP get response PDUs generated by SNMP.
<code>out traps</code>	Displays the number of SNMP Trap PDUs generated by SNMP.
<code>variables requested</code>	Displays the number of MIB objects requested by SNMP.
<code>variables set</code>	Displays the number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs.

Sample Output

```
A:ALA-1# show snmp counters
=====
SNMP counters:
=====
  in packets : 463
```

```

-----
      in gets      : 93
      in getnexts : 0
      in sets     : 370
      out packets: 463
-----
      out get responses : 463
      out traps        : 0
      variables requested: 33
      variables set     : 497
=====
A:ALA-1#

```

information

- Syntax** **information**
- Context** show>system
- Description** This command lists the SNMP configuration and statistics.
- Output** **System Information Output Fields** — The following table describes system information output fields.

Table 17: Show System Information Output Fields

Label	Description
System Name	The name configured for the device.
System Contact	The text string that identifies the contact name for the device.
System Location	The text string that identifies the location of the device.
System Coordinates	The text string that identifies the system coordinates for the device location. For example, "37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.
System Up Time	The time since the last reboot.
SNMP Port	The port which SNMP sends responses to management requests.
SNMP Engine ID	The ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node.
SNMP Max Message Size	The maximum size SNMP packet generated by this node.
SNMP Admin State	Enabled — SNMP is administratively enabled. Disabled — SNMP is administratively disabled.
SNMP Oper State	Enabled — SNMP is operationally enabled. Disabled — SNMP is operationally disabled.

Table 17: Show System Information Output Fields (Continued)

Label	Description
SNMP Index Boot Status	<p><code>Persistent</code> – Persistent indexes at the last system reboot was enabled.</p> <p><code>Disabled</code> – Persistent indexes at the last system reboot was disabled.</p>
SNMP Sync State	The state when the synchronization of configuration files between the primary and secondary s finish.
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 boot location of the BOF.
Image Source	<p><code>primary</code> – Specifies whether the image was loaded from the primary location specified in the BOF.</p> <p><code>secondary</code> – Specifies whether the image was loaded from the secondary location specified in the BOF.</p> <p><code>tertiary</code> – Specifies whether the image was loaded from the tertiary location specified in the BOF.</p>
Config Source	<p><code>primary</code> – Specifies whether the configuration was loaded from the primary location specified in the BOF.</p> <p><code>secondary</code> – Specifies whether the configuration was loaded from the secondary location specified in the BOF.</p> <p><code>tertiary</code> – Specifies whether the configuration was loaded from the tertiary location specified in the BOF.</p>
Last Booted Config File	Displays the URL and filename of the configuration file used for the most recent boot.
Last Boot Cfg Version	Displays the version of the configuration file used for the most recent boot.
Last Boot Config Header	Displays header information of the configuration file used for the most recent boot.
Last Boot Index Version	Displays the index version used in the most recent boot.
Last Boot Index Header	Displays the header information of the index used in the most recent boot.
Last Saved Config	Displays the filename of the last saved configuration.

Table 17: Show System Information Output Fields (Continued)

Label	Description
Time Last Saved	Displays the time the configuration was most recently saved.
Changes Since Last Save	Yes – The configuration changed since the last save. No – The configuration has not changed since the last save.
Time Last Modified	Displays the time of the last modification.
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL – The location and name of the CLI script file executed following successful completion of the boot-up configuration file execution. N/A – No CLI script file is executed.
Cfg-OK Script Status	Successful/Failed – The results from the execution of the CLI script file specified in the Cfg-OK Script location. Not used – No CLI script file was executed.
Cfg-Fail Script	URL – The location and name of the CLI script file executed following a failed boot-up configuration file execution. Not used – No CLI script file was executed.
Cfg-Fail Script Status	Successful/Failed – The results from the execution of the CLI script file specified in the Cfg-Fail Script location. Not used – No CLI script file was executed.
Management IP address	The Management IP address of the node.
DNS Server	The DNS address of the node.
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.

Sample Output

```

A:ALA-1# show system information
=====
System Information
=====
System Name           : ALA-1
System Type           :
System Version        : B-0.0.I1204
System Contact        :
System Location       :
System Coordinates    :
System Active Slot    : A
System Up Time        : 1 days, 02:12:57.84 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f00000479ff000000
SNMP Max Message Size : 1500
SNMP Admin State      : Enabled
SNMP Oper State       : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State       : OK

Telnet/SSH/FTP Admin  : Enabled/Enabled/Disabled
Telnet/SSH/FTP Oper   : Up/Up/Down

BOF Source            : cf1:
Image Source          : primary
Config Source         : primary
Last Booted Config File: ftp://172.22.184.249/./debby-sim1/debby-sim1-config.cfg
Last Boot Cfg Version : THU FEB 15 16:58:20 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                        Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                        reserved. All use subject to applicable license
                        agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                        builder in /rel0.0/I1042/panos/main # Generated THU
                        FEB 11 16:58:20 2007 UTC

Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                        Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                        reserved. All use subject to applicable license
                        agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                        builder in /rel0.0/I1042/panos/main # Generated THU
                        FEB 15 16:58:20 2007 UTC

Last Saved Config     : N/A
Time Last Saved       : N/A
Changes Since Last Save: No
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script         : N/A
Cfg-OK Script Status  : not used
Cfg-Fail Script       : N/A
Cfg-Fail Script Status : not used

Management IP Addr    : 192.168.2.121/20
DNS Server            : 192.168.1.246
DNS Domain            : eng.timetra.com
BOF Static Routes     :

```



```

snmp-rw          snmpv2c  none      no-security  no-security  no-security
snmp-rwa        snmpv1    none      iso          iso          iso
snmp-rwa        snmpv2c  none      iso          iso          iso
snmp-trap       snmpv1    none      iso          iso          iso
snmp-trap       snmpv2c  none      iso          iso          iso
-----
No. of Access Groups: 8
=====
A:ALA-1#

A:ALA-1# show system security access-group detail
=====
Access Groups
=====
group name      security  security  read      write      notify
                model     level     view      view      view
-----
snmp-ro        snmpv1   none      no-security  no-security  no-security
-----
No. of Access Groups:
...
=====
A:ALA-1#

```

authentication

Syntax	authentication [statistics]
Context	show>system>security
Description	This command displays authentication information.
Output	Authentication Output — The following table describes the authentication output fields.

Label	Description
sequence	The authentication order in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.
server address	The address of the RADIUS, TACACS+, or local server.
status	The status of the server.
type	The type of server.
timeout (secs)	Number of seconds the server will wait before timing out.
single connection	Specifies whether a single connection is established with the server. The connection is kept open and is used by all the TELNET/SSH/FTP sessions for AAA operations.
retry count	The number of attempts to retry contacting the server.

Label	Description
radius admin status	The administrative status of the RADIUS protocol operation.
tacplus admin status	The administrative status of the TACACS+ protocol operation.
health check	Specifies whether the RADIUS and TACACS+ servers will be periodically monitored. Each server will be contacted every 30 seconds. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent.
No. of Servers	The total number of servers configured.

Sample Output

```
A:ALA-49>show>system>security# authentication
=====
Authentication                sequence : radius tacplus local
=====
server address  status  type    timeout(secs)  single connection  retry count
-----
10.10.10.103   up      radius  5              n/a                 5
10.10.0.1      up      radius  5              n/a                 5
10.10.0.2      up      radius  5              n/a                 5
10.10.0.3      up      radius  5              n/a                 5
-----
radius admin status : down
tacplus admin status : up
health check        : enabled
-----
No. of Servers: 4
=====
A:ALA-49>show>system>security#
```

communities

- Syntax** communities
- Context** show>system>security
- Description** This command lists SNMP communities and characteristics.
- Output** **Communities Ouput** — The following table describes the communities output fields.

Sample Output**Table 19: Show Communities Output Fields**

Label	Description
Community	The community string name for SNMPv1 and SNMPv2c access only.
Access	r – The community string allows read-only access. rw – The community string allows read-write access. rwa – The community string allows read-write access.
View	mgmt – The unique SNMP community string assigned to the management router.
Version	The view name.
Group Name	The SNMP version.
No of Communities	The access group name.
	The total number of configured community strings.

```
A:ALA-1# show system security communities
=====
Communities
=====
community      access  view          version  group name
-----
private        rw      iso           v1 v2c   snmp-rwa
public         r       no-security   v1 v2c   snmp-ro
rwa            rwa     n/a           v2c      snmp-trap
-----
No. of Communities: 3
=====
A:ALA-1#
```

keychain

- Syntax** **keychain** [*key-chain*] [**detail**]
- Context** show>system>security
- Description** This command displays keychain information.
- Parameters** *key-chain* — Specifies the keychain name to display.
detail — Displays detailed keychain information.
- Output** *A:ALA-A# show system security keychain test

```
=====
Key chain:test
=====
```

Show Commands

```
TCP-Option number send : 254 Admin state : Up
TCP-Option number receive : 254 Oper state : Up
=====
*A:ALA-A#
```

management-access-filter

- Syntax** `management-access-filter`
- Context** `show>system>security`
- Description** This command displays management access filter information for IP and MAC filters.

ip-filter

- Syntax** `ip-filter [entry entry-id]`
- Context** `show>system>security>mgmt-access-filter`
- Description** this command displays management-access IP filters.
- Parameters** *entry-id* — Displays information for the specified entry.

Values 1 — 9999

Output Management Access Filter Output — The following table describes management access filter output fields.

Table 20: Show Management Access Filter Output Fields

Label	Description
Def. action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted. Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued. Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied.
Entry	The entry ID in a policy or filter table.
Description	A text string describing the filter.
Src IP	The source IP address used for management access filter match criteria.
Src Interface	The interface name for the next-hop to which the packet should be forwarded if it hits this filter entry.
Dest port	The destination port.

Table 20: Show Management Access Filter Output Fields (Continued)

Label	Description
Match	The number of times a management packet has matched this filter entry.
Protocol	The IP protocol to match.
Action	The action to take for packets that match this filter entry.

```

Output *7210-SAS>show>system>security>management-access-filter# ip-filter entry 1

=====
IPv4 Management Access Filter
=====
filter type      : ip
Def. Action      : permit
Admin Status     : enabled (no shutdown)
-----
Entry            : 1
Description      : (Not Specified)
Src IP           : undefined
Src interface    : undefined
Dest port        : undefined
Protocol         : undefined
Router           : undefined
Action           : none
Log              : disabled
Matches          : 0
=====
*7210-SAS>show>system>security>management-access-filter#

```

password-options

- Syntax** password-options
- Context** show>system>security
- Description** This command displays password options.
- Output** **Password-Options Output** — The following table describes password-options output fields.

Label	Description
Password aging in days	Number of days a user password is valid before the user must change his password.
Number of invalid attempts permitted per login	Displays the maximum number of unsuccessful login attempts allowed for a user.

Label	Description
Time in minutes per login attempt	Displays the time in minutes that user is to be locked out.
Lockout period (when threshold breached)	Displays the number of minutes the user is locked out if the threshold of unsuccessful login attempts has exceeded.
Authentication order	Displays the most preferred method to authenticate and authorize a user.
Configured complexity options	Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the authentication section.
Minimum password length	Displays the minimum number of characters required in the password.

Sample Output

```
A:ALA-48>show>system>security# password-options
=====
Password Options
=====
Password aging in days                : 365
Number of invalid attempts permitted per login : 5
Time in minutes per login attempt      : 5
Lockout period (when threshold breached) : 20
Authentication order                  : radius tacplus local
Configured complexity options          :
Minimum password length                : 8
=====
A:ALA-48>show>system>security#
```

profile

- Syntax** **profile** [*profile-name*]
- Context** show>system>security
- Description** This command displays user profiles for CLI command tree permissions.
- Parameters** *profile-name* — Specify the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names are listed.

Output Profile Output — The following table describes the profile output fields.

Label	Description
User Profile	<p><code>default</code> — The action to be given to the user profile if none of the entries match the command.</p> <p><code>administrative</code> — specifies the administrative state for this profile.</p>
Def. Action	<p><code>none</code> — No action is given to the user profile when none of the entries match the command.</p> <p><code>permit-all</code> — The action to be taken when an entry matches the command.</p>
Entry	<p>10 - 80 — Each entry represents the configuration for a system user.</p>
Description	<p>A text string describing the entry.</p>
Match Command	<p><code>administrative</code> — Enables the user to execute all commands.</p> <p><code>configure system security</code> — Enables the user to execute the config system security command.</p> <p><code>enable-admin</code> — Enables the user to enter a special administrative mode by entering the enable-admin command.</p> <p><code>exec</code> — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console.</p> <p><code>exit</code> — Enables the user to execute the exit command.</p> <p><code>help</code> — Enables the user to execute the help command.</p> <p><code>logout</code> — Enables the user to execute the logout command.</p> <p><code>password</code> — Enables the user to execute the password command.</p> <p><code>show config</code> — Enables the user to execute the show config command.</p> <p><code>show</code> — Enables the user to execute the show command.</p> <p><code>show system security</code> — Enables the user to execute the show system security command.</p>
Action	<p><code>permit</code> — Enables the user access to all commands.</p> <p><code>deny-all</code> — Denies the user access to all commands.</p>

```
A:ALA-48>config>system>snmp# show system security profile
```

```
=====
```

Show Commands

```
User Profile
=====
User Profile : test
Def. Action  : none
-----
Entry       : 1
Description :
Match Command:
Action      : unknown
=====
User Profile : default
Def. Action  : none
-----
Entry       : 10
Description :
Match Command: exec
Action      : permit
-----
Entry       : 20
Description :
Match Command: exit
Action      : permit
-----
Entry       : 30
Description :
Match Command: help
Action      : permit
-----
...
-----
Entry       : 80
Description :
Match Command: enable-admin
Action      : permit
=====

User Profile : administrative
Def. Action  : permit-all
-----
Entry       : 10
Description :
Match Command: configure system security
Action      : permit
-----
Entry       : 20
Description :
Match Command: show system security
Action      : permit
=====
-----
No. of profiles: 3
=====
A:ALA-48>config>system>snmp#
```

ssh

- Syntax** `ssh`
- Context** `show>system>security`
- Description** This command displays all the SSH sessions as well as the SSH status and fingerprint.
- Output** **SSH Options Output** — The following table describes SSH output fields.

Table 21: Show SSH Output Fields

Label	Description
SSH status	SSH is enabled — Displays that SSH server is enabled. SSH is disabled — Displays that SSH server is disabled.
Key fingerprint	The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected router(s) (remote client).
Encryption	des — Data encryption using a private (secret) key. 3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.
Username	The name of the user.
Number of SSH sessions	The total number of SSH sessions.

Sample output

```
A:ALA-7# show system security ssh
SSH is enabled
Key fingerprint: 34:00:f4:97:05:71:aa:b1:63:99:dc:17:11:73:43:83
=====
Connection      Encryption      Username
=====
192.168.5.218    3des           admin
-----
Number of SSH sessions : 1
=====
A:ALA-7#

A:ALA-49>config>system>security# show system security ssh

SSH is disabled

A:ALA-49>config>system>security#
```

user

Syntax `users [user-id] [detail]`

Context `show>system>security`

Description This command displays user information.

Output **User Output** — The following table describes user information output fields.

Table 22: Show User Output Fields

Label	Description
User ID	The name of a system user.
Need New PWD	Yes — The user must change his password at the next login.
	No — The user is not forced to change his password at the next login.
User Permission	Console — Specifies whether the user is permitted console/Telnet access.
	FTP — Specifies whether the user is permitted FTP access.
	SNMP — Specifies whether the user is permitted SNMP access.
Password expires	The date on which the current password expires.
Attempted logins	The number of times the user has attempted to login irrespective of whether the login succeeded or failed.
Failed logins	The number of unsuccessful login attempts.
Local Conf.	Y — Password authentication is based on the local password database.
	N — Password authentication is not based on the local password database.

Sample Output

```
A:ALA-1# show system security user
=====
Users
=====
user id          need   user permissions password  attempted failed  local
                  new pwd console ftp snmp  expires  logins  logins  conf
-----
admin            n     y      n  n    never    2       0       y
testuser        n     n      n  y    never    0       0       y
-----
Number of users : 2
=====
A:ALA-1#
```

view

Syntax `view [view-name] [detail]`

Context `show>system>security`

Description This command lists one or all views and permissions in the MIB-OID tree.

Output **System Security View Output** — The following table describes system security view output fields.

Table 23: Show System Security View Output Fields

Label	Description
View name	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.
OID tree	The Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.
Mask	The mask value and the mask type, along with the <i>oid-value</i> configured in the view command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.
Permission	Included — Specifies to include MIB subtree objects. Excluded — Specifies to exclude MIB subtree objects.
No. of Views	The total number of configured views.
Group name	The access group name.

Sample Output

```
A:ALA-1# show system security view
=====
Views
=====
view name      oid tree      mask          permission
-----
iso            1             included
no-security    1             included
no-security    1.3.6.1.6.3   excluded
no-security    1.3.6.1.6.3.10.2.1 included
no-security    1.3.6.1.6.3.11.2.1 included
no-security    1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 6
=====
A:ALA-1#
```

Show Commands

```
A:ALA-1# show system security view no-security detail
=====
Views
=====
view name          oid tree          mask          permission
-----
no-security        1                included
no-security        1.3.6.1.6.3      excluded
no-security        1.3.6.1.6.3.10.2.1 included
no-security        1.3.6.1.6.3.11.2.1 included
no-security        1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 5
=====
no-security used in
=====
group name
-----
snmp-ro
snmp-rw
=====
A:ALA-1#
```

Event and Accounting Logs

In This Chapter

This chapter provides information about configuring event and accounting logs in the 7210 SAS.

Topics in this chapter include:

- [Logging Overview on page 212](#)
- [Log Destinations on page 214](#)
- [Event Logs on page 219](#)
 - [Event Sources on page 220](#)
 - [Event Control on page 222](#)
 - [Log Manager and Event Logs on page 224](#)
 - [Event Filter Policies on page 225](#)
 - [Event Log Entries on page 226](#)
 - [Simple Logger Event Throttling on page 228](#)
 - [Default System Log on page 229](#)
- [Accounting Logs on page 230](#)
 - [Accounting Records on page 230](#)
- [Configuration Notes on page 270](#)

Logging Overview

The two primary types of logging supported in the 7210 SAS OS are event logging and accounting logs.

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The 7210 SAS groups events into three major categories or event sources:

- Security events — Events that pertain to attempts to breach system security.
- Change events — Events that pertain to the configuration and operation of the node.
- Main events — Events that pertain to applications that are not assigned to other event categories/sources.
- Debug events — Events that pertain to trace or other debugging information.

The following are events within the 7210 SAS and have the following characteristics:

- A time stamp in UTC or local time.
- The generating application.
- A unique event ID within the application.
- The VRF-ID.
- A subject identifying the affected object.
- A short text description.

Event control assigns the severity for each application event and whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7210 SAS OS conform to ITU standards M.3100 X.733 and X.21 and are listed in [Table 24](#).

Table 24: Event Severity Levels

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Events that are suppressed by event control will not generate any event log entries. Event control maintains a count of the number of events generated (logged) and dropped (suppressed) for each application event. The severity of an application event can be configured in event control.

An event log within the 7210 SAS OS associates the event sources with logging destinations. Examples of logging destinations include, the console session, a specific telnet or SSH session, memory logs, file destinations, SNMP trap groups and syslog destinations. A log filter policy can be associated with the event log to control which events will be logged in the event log based on combinations of application, severity, event ID range, VRF ID, and the subject of the event.

The 7210 SAS accounting logs collect comprehensive accounting statistics to support a variety of billing models. The routers collect accounting data on services and network ports on a per-service class basis. In addition to gathering information critical for service billing, accounting records can be analyzed to provide insight about customer service trends for potential service revenue opportunities. Accounting statistics on network ports can be used to track link utilization and network traffic pattern trends. This information is valuable for traffic engineering and capacity planning within the network core.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to access objects (such as access ports and SAPs or network objects (such as SDPs, network ports, network IP interface). Accounting statistics are collected by counters for individual service meters defined on the customer's SAP or by the counters within forwarding class (FC) queues defined on the network ports.

The type of record defined within the accounting policy determines where a policy is applied, what statistics are collected and time interval at which to collect statistics.

The "location" field of the file-id lets the user configure the device and store it in any directory. The default value is cf1:, but it can also be uf1: (for devices supporting USB) and uf1: and cf2: for 7210 SAS-T

Log Destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. 7210 SAS-Series devices support the following log destinations:

- [Console on page 214](#)
- [Session on page 214](#)
- [Memory Logs on page 214](#)
- [Log Files on page 215](#)
- [SNMP Trap Group on page 217](#)
- [Syslog on page 217](#)

Only a single log destination can be associated with an event log or with an accounting log. An event log can be associated with multiple event sources, but it can only have a single log destination.

A file destination is the only type of log destination that can be configured for an accounting log.

Console

Sending events to a console destination means the message will be sent to the system console. The console device can be used as an event log destination.

Session

A session destination is a temporary log destination which directs entries to the active telnet or SSH session for the duration of the session. When the session is terminated, for example, when the user logs out, the event log is removed. Event logs configured with a session destination are not stored in the configuration file. Event logs can direct log entries to the session destination.

Memory Logs

A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it can hold can be specified, otherwise it will assume a default size. An event log can send entries to a memory log destination.

Log Files

Log files can be used by both event logs and accounting logs and are stored on the compact flash devices (specifically cf1:) in the file system.

A log file is identified with a single log file ID, but a log file will generally be composed of a number individual files in the file system. A log file is configured with a rollover parameter, expressed in minutes, which represents the length of time an individual log file should be written to before a new file is created for the relevant log file ID. The rollover time is checked only when an update to the log is performed. Thus, complying to this rule is subject to the incoming rate of the data being logged. For example, if the rate is very low, the actual rollover time may be longer than the configured value.

The retention time for a log file specifies the amount of time the file should be retained on the system based on the creation date and time of the file. The system continuously checks for log files with expired retention periods once every hour and deletes as many files as possible during a ten second interval.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file.

Event log files are always created in the **\log** directory on the specified compact flash device. The naming convention for event log files is:

```
log eeff-timestamp
```

where:

ee is the event log ID

ff is the log file destination ID

timestamp is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

yyyy is the four-digit year (for example, 2007)

mm is the two digit number representing the month (for example, 12 for December)

dd is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

hh is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

mm is the two digit minute (for example, 30 for 30 minutes past the hour)

ss is the two digit second (for example, 14 for 14 seconds)

Log Destinations

Accounting log files are created in the `\act-collect` directory on a compact flash device (*cfI*). The naming convention for accounting log files is nearly the same as for log files except the prefix **act** is used instead of the prefix **log**. The naming convention for accounting logs is:

```
act aa $ff$ -timestamp.xml.gz
```

where:

aa is the accounting policy ID

ff is the log file destination ID

timestamp is the timestamp when the file is created in the form of *yyyymmdd-hhmmss*
where:

yyyy is the four-digit year (for example, 2007)

mm is the two digit number representing the month (for example, 12 for December)

dd is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

hh is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

mm is the two digit minute (for example, 30 for 30 minutes past the hour)

ss is the two digit second (for example, 14 for 14 seconds)

Accounting logs are `.xml` files created in a compressed format and have a `.gz` extension.

The `\act-collect` directory is where active accounting logs are written. When an accounting log is rolled over, the active file is closed and archived in the `\act` directory before a new active accounting log file created in `\act-collect`.

SNMP Trap Group

An event log can be configured to send events to SNMP trap receivers by specifying an SNMP trap group destination.

An SNMP trap group can have multiple trap targets. Each trap target can have different operational parameters.

A trap destination has the following properties:

- The IP address of the trap receiver.
- The UDP port used to send the SNMP trap.
- SNMP version (v1, v2c, or v3) used to format the SNMP notification.
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

For SNMP traps that will be sent in-band, the source IP address of the trap is the system IP address of the 7210 SAS.

Each trap target destination of a trap group receives the identical sequence of events as defined by the log ID and the associated sources and log filter applied.

Syslog

An event log can be configured to send events to one syslog destination. Syslog destinations have the following properties:

- Syslog server IP address.
- The UDP port used to send the syslog message.
- The Syslog Facility Code (0 - 23) (default 23 - local 7).
- The Syslog Severity Threshold (0 - 7) - events exceeding the configured level will be sent.

Because syslog uses eight severity levels whereas the 7210 SAS-Series uses six internal severity levels, the severity levels are mapped to syslog severities. [Table 25](#) displays the severity level mappings to syslog severities.

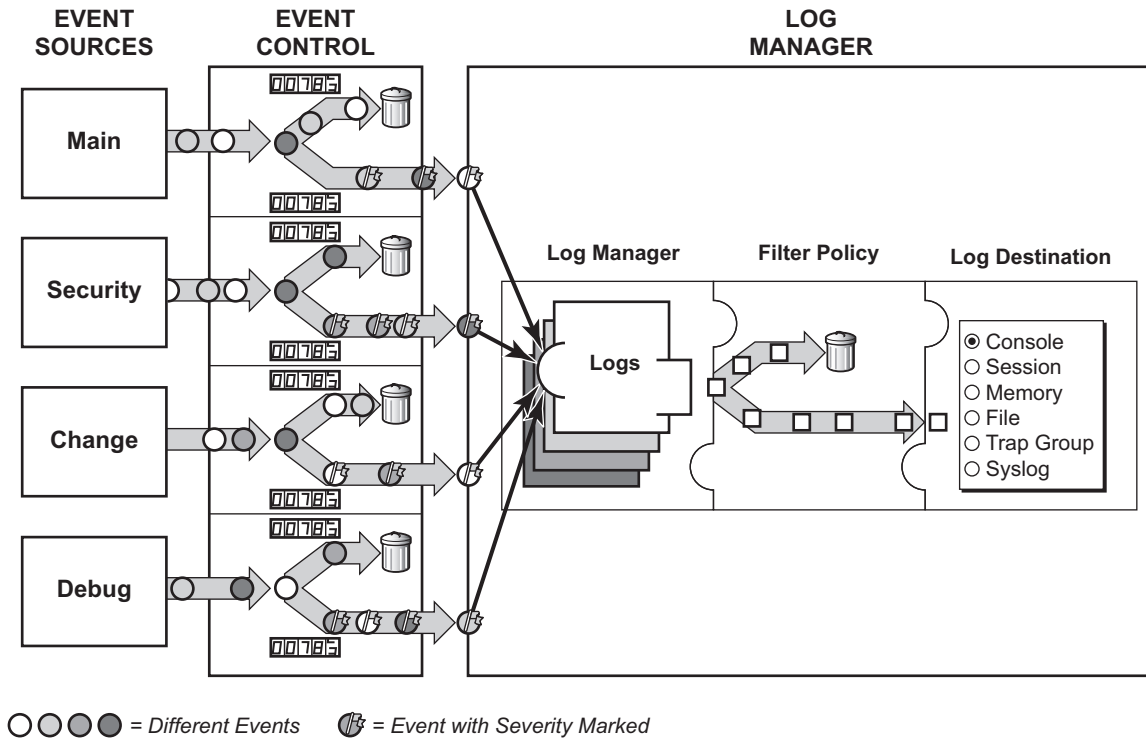
Table 25: 7210 SAS-Series to Syslog Severity Level Mappings

Severity Level	Numerical Severity (highest to lowest)	Syslog Configured Severity	Definition
	0	emergency	System is unusable
3	1	alert	Action must be taken immediately
4	2	critical	Critical conditions
5	3	error	Error conditions
6	4	warning	Warning conditions
	5	notice	Normal but significant condition
1 cleared 2 indeterminate	6	info	Informational messages
	7	debug	Debug-level messages

Event Logs

Event logs are the means of recording system generated events for later analysis. Events are messages generated by the system by applications or processes within the 7210 SAS.

Figure 4 depicts a function block diagram of event logging.



CLI0001B

Figure 4: Event Logging Block Diagram

Event Sources

In [Figure 4](#), the event sources are the main categories of events that feed the log manager.

- Security — The security event source is all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the SECURITY application and the authenticationFailure event in the SNMP application.
- Change — The change activity event source is all events that directly affect the configuration or operation of the node. Change events are generated by the USER application. The Change event stream also includes the tmnxConfigModify(#2006), tmnxConfigCreate (#2007), tmnxConfigDelete (#2008) and tmnxStateChange (#2009) change events from the SYSTEM application.
- Debug — The debug event source is the debugging configuration that has been enabled on the system. Debug events are generated by the DEBUG application.
- Main — The main event source receives events from all other applications within the 7210 SAS.

Examples of applications within 7210 SAS include IP, MPLS, OSPF, CLI, services, etc. [Figure 5](#) displays an example of the **show log applications** command output which displays all applications.

```
*A:ALU-7210# show log applications
=====
Log Event Application Names
=====
Application Name
-----
CHASSIS
DEBUG
DOT1AG
DOT1X
EFM_OAM
FILTER
IGMP
IP
LAG
LOGGER
MIRROR
NTP
OAM
PORT
QOS
SECURITY
SNMP
STP
SVCNMR
SYSTEM
TIP
TOD
USER
VRTR
=====
*A:ALU-7210#
```

Figure 5: Show Log Applications Command Output

Event Control

Event control pre-processes the events generated by applications before the event is passed into the main event stream. Event control assigns a severity to application events and can either forward the event to the main event source or suppress the event. Suppressed events are counted in event control, but these events will not generate log entries as it never reaches the log manager.

Simple event throttling is another method of event control and is configured similarly to the generation and suppression options. See [Simple Logger Event Throttling on page 228](#).

Events are assigned a default severity level in the system, but the application event severities can be changed by the user.

Application events contain an event number and description that explains why the event is generated. The event number is unique within an application, but the number can be duplicated in other applications.

The following example, generated by querying event control for application generated events, displays a partial list of event numbers and names.

```
router# show log event-control
=====
Log Events
=====
Application
ID#      Event Name                               P   g/s   Logged   Dropped
-----
CHASSIS:
  2001  cardFailure                             MA  gen    0         0
  2002  cardInserted                            MI  gen    2         0
  2003  cardRemoved                             MI  gen    0         0
  2004  cardWrong                               MI  gen    0         0
  2005  EnvTemperatureTooHigh                   MA  gen    0         0
  2006  fanFailure                              CR  gen    0         0
  ...
EFM_OAM:
  2001  tmnxDot3OamPeerChanged                  MI  gen    0         0
  2002  tmnxDot3OamLoopDetected                 MI  gen    0         0
  2003  tmnxDot3OamLoopCleared                  MI  gen    0         0
FILTER:
  2001  tIPFilterPBRPacketsDrop                  WA  gen    0         0
  2002  tFilterEntryActivationFailed             WA  gen    0         0
  2003  tFilterEntryActivationRestored           WA  gen    0         0
IGMP:
  2001  vRtrIcmpIfRxQueryVerMismatch            WA  gen    0         0
  2002  vRtrIcmpIfCModeRxQueryMismatch          WA  gen    0         0
  2003  vRtrIcmpMaxGrpsLimitExceeded            WA  gen    0         0
  2004  vRtrIcmpMcacPlyDropped                  WA  gen    0         0
IP:
L  2001  clearRTMError                           MI  gen    0         0
L  2002  ipEtherBroadcast                         MI  gen    0         0
L  2003  ipDuplicateAddress                       MI  gen    0         0
L  2004  ipArpInfoOverwritten                     MI  gen    0         0
```

Event and Accounting Logs

```
L 2005 fibAddFailed          MA gen          0          0
...
SYSTEM:
  2001 stiDateAndTimeChanged  WA gen          0          0
  2002 ssiSaveConfigSucceeded MA gen          1          0
  2003 ssiSaveConfigFailed   CR gen          1          0
  2004 sbiBootConfig         MA gen          1          0
  2005 sbiBootSnmpd         MA gen          1          0
...
VRTR:
  2001 tmnxVRtrMidRouteTCA    MI gen          0          0
  2002 tmnxVRtrHighRouteTCA  MI gen          0          0
  2003 tmnxVRtrHighRouteCleared MI gen          0          0
...
=====
router#
```

Log Manager and Event Logs

Events that are forwarded by event control are sent to the log manager. The log manager manages the event logs in the system and the relationships between the log sources, event logs and log destinations, and log filter policies.

An event log has the following properties:

- A unique log ID
The log ID is a short, numeric identifier for the event log. A maximum of ten logs can be configured at a time.
- One or more log sources
The source stream or streams to be sent to log destinations can be specified. The source must be identified before the destination can be specified. The events can be from the main event stream, events in the security event stream, or events in the user activity stream.
- One event log destination
A log can only have a single destination. The destination for the log ID destination can be one of console, session, syslog, snmp-trap-group, memory, or a file on the local file system.
- An optional event filter policy
An event filter policy defines whether to forward or drop an event or trap-based on match criteria.

Event Filter Policies

The log manager uses event filter policies to allow fine control over which events are forwarded or dropped based on various criteria. Like other policies with the 7210 SAS, filter policies have a default action. The default actions are either:

- Forward
- Drop

Filter policies also include a number of filter policy entries that are identified with an entry ID and define specific match criteria and a forward or drop action for the match criteria.

Each entry contains a combination of matching criteria that define the application, event number, router, severity, and subject conditions. The entry's action determines how the packets should be treated if they have met the match criteria.

Entries are evaluated in order from the lowest to the highest entry ID. The first matching event is subject to the forward or drop action for that entry.

Valid operators are displayed in [Table 26](#):

Table 26: Valid Filter Policy Operators

Operator	Description
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

A match criteria entry can include combinations of:

- Equal to or not equal to a given system application.
- Equal to, not equal to, less than, less than or equal to, greater than or greater than or equal to an event number within the application.
- Equal to, not equal to, less than, less than or equal to, greater than or greater than or equal to a severity level.
- Equal to or not equal to a router name string or regular expression match.
- Equal to or not equal to an event subject string or regular expression match.

Event Log Entries

Log entries that are forwarded to a destination are formatted in a way appropriate for the specific destination whether it be recorded to a file or sent as an SNMP trap, but log event entries have common elements or properties. All application generated events have the following properties:

- A time stamp in UTC or local time.
- The generating application.
- A unique event ID within the application.
- A router name identifying the VRF-ID that generated the event.
- A subject identifying the affected object.
- A short text description.

The general format for an event in an event log with either a memory, console or file destination is as follows.

```
nnnn YYYY/MM/DD HH:MM:SS.SS <severity>:<application> # <event_id> <router-name> <subject>
description
```

The following is an event log example:

```
475 2006/11/27 00:19:40.38 WARNING: SNMP #2007 Base 1/1/1
"interface 1/1/1 came up"
```

The specific elements that compose the general format are described in [Table 27](#).

Table 27: Log Entry Field Descriptions

Label	Description
nnnn	The log entry sequence number.
YYYY/MM/DD	The UTC date stamp for the log entry. <i>YYYY</i> — Year <i>MM</i> — Month <i>DD</i> — Date
HH:MM:SS.SS	The UTC time stamp for the event. <i>HH</i> — Hours (24 hour format) <i>MM</i> — Minutes <i>SS.SS</i> — Seconds

Table 27: Log Entry Field Descriptions (Continued)

Label	Description
<severity>	The severity level name of the event. CLEARED — A cleared event (severity number 1). INFO — An indeterminate/informational severity event (severity level 2). CRITICAL — A critical severity event (severity level 3). MAJOR — A major severity event (severity level 4). MINOR — A minor severity event (severity level 5). WARNING — A warning severity event (severity 6).
<application>	The application generating the log message.
<event_id>	The application's event ID number for the event.
<router>	The router name representing the VRF-ID that generated the event.
<subject>	The subject/affected object for the event.
<description>	A text description of the event.

Simple Logger Event Throttling

Simple event throttling provides a mechanism to protect event receivers from being overloaded when a scenario causes many events to be generated in a very short period of time. A throttling rate, # events/# seconds, can be configured. Specific event types can be configured to be throttled. Once the throttling event limit is exceeded in a throttling interval, any further events of that type cause the dropped events counter to be incremented. Dropped events counts are displayed by the **show>log>event-control** context. Events are dropped before being sent to one of the logger event collector tasks. There is no record of the details of the dropped events and therefore no way to retrieve event history data lost by this throttling method.

A particular event type can be generated by multiple managed objects within the system. At the point this throttling method is applied the logger application has no information about the managed object that generated the event and cannot distinguish between events generated by object "A" from events generated by object "B". If the events have the same event-id, they are throttled regardless of the managed object that generated them. It also does not know which events may eventually be logged to destination log-id <n> from events that will be logged to destination log-id <m>.

Throttle rate applies commonly to all event types. It is not configurable for a specific event-type.

A timer task checks for events dropped by throttling when the throttle interval expires. If any events have been dropped, a TIMETRA-SYSTEM-MIB::tmnxTrapDropped notification is sent.

Default System Log

Log 99 is a pre-configured memory-based log which logs events from the main event source (not security, debug, etc.). Log 99 exists by default.

The following example displays the log 99 configuration.

```
ALA-1>config>log# info detail
#-----
echo "Log Configuration "
#-----
...
    snmp-trap-group 7
    exit
...
    log-id 99
        description "Default system log"
        no filter
        from main
        to memory 500
        no shutdown
    exit
-----
ALA-1>config>log#
```

Accounting Logs

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory on compact flash (*cfl:*) in a compressed (tar) XML format and can be retrieved using FTP or SCP.

A file ID can only be assigned to either one event log ID or one accounting log.

Accounting Records

An accounting policy must define a record name and collection interval. Only one record name can be configured per accounting policy. Also, a record name can only be used in one accounting policy.

The record name, sub-record types, and default collection period for access and network accounting policies are shown below.

Table 28: Accounting Record Names and Collection Periods

Accounting-Record-Names	Sub-Record types	Accounting-Object	Default Collection Interval (In minutes)	Supported modes
service-ingress-octets	sio	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
service-egress-octets	seo	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
service-ingress-packets	sip	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
service-egress-packets	sep	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network

Table 28: Accounting Record Names and Collection Periods (Continued)

Accounting-Record-Names	Sub-Record types	Accounting-Object	Default Collection Interval (In minutes)	Supported modes
combined-service-ingress	sio,sip	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
combined-service-egress	seo,sep	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
complete-service-ingress-egress	sio,sip,seo,sep	sap	5	<ul style="list-style-type: none"> • Access Uplink • Network
access-egress-packets(not supported on 7210 SAS-X)	aep	access-port	5	<ul style="list-style-type: none"> • Access Uplink • Network
access-egress-octets (not supported on 7210 SAS-X)	aeo	access-port	5	<ul style="list-style-type: none"> • Access Uplink • Network
combined-access-egress (not supported on 7210 SAS-X)	cmAeo,cmAep	access-port	5	<ul style="list-style-type: none"> • Access Uplink • Network
network-ingress-octets	nio	network-port	15	<ul style="list-style-type: none"> • Access Uplink • Network
network-ingress-packets	nip	network-port	15	<ul style="list-style-type: none"> • Access Uplink • Network
network-egress-octets	neo	network-port	15	<ul style="list-style-type: none"> • Access Uplink • Network
network-egress-packets	nep	network-port	15	<ul style="list-style-type: none"> • Access Uplink • Network

Table 28: Accounting Record Names and Collection Periods (Continued)

Accounting-Record-Names	Sub-Record types	Accounting-Object	Default Collection Interval (In minutes)	Supported modes
combined-network-egress	cmNeo,cmNep	network-port	15	<ul style="list-style-type: none"> Access Uplink Network
combined-network-ingress-egress-octets	cmNio,cmNeo	network-port	15	<ul style="list-style-type: none"> Access Uplink Network
network-interface-ingress-octets	niio	IP Interface	15	<ul style="list-style-type: none"> Network
network-interface-ingress-packets	niip	IP Interface	15	<ul style="list-style-type: none"> Network
combined-network-interface-ingress	niio,niip	IP Interface	15	<ul style="list-style-type: none"> Network
combined-sdp-ingress-egress	cmSdpipo,cmSdpepo	sdp spoke-sdp	5	<ul style="list-style-type: none"> Network
complete-sdp-ingress-egress	cmSdpipo,cmSdpepo,cpSdpipo,cpSdpepo	sdp spoke-sdp	5	<ul style="list-style-type: none"> Network

In the 7210 SAS, a total of 21 accounting-records are available. There are five types of accounting policies:

- access
- accessport
- network
- networkIf
- sdp

NOTE: Not all the above accounting records and counters per record are supported on all the 7210 platforms. The list of accounting records and counters per record supported for each of the 7210 platform in different modes is listed below. Please use that to know the support available on different 7210 platforms.

When creating accounting policies, only one (of each) access, accessport, network, networkIf and sdp accounting-policy can be defined as default. If statistics collection is enabled on an accounting

object, and no accounting policy is applied, then the respective default accounting policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Each accounting record name is composed of one or more sub-records which is composed of multiple fields.

In 7210 SAS devices for VLL and VPLS services, the counter-mode of counters associated SAP ingress meters or policers can be changed by executing the command **config>service>epipe/vpls>sap>statistics>ingress>counter-mode{in-out-profile-count|forward-drop-count}**. (For more information on the counter-mode command refer to the 7210 SAS-M, T, Mxp, Sx Services guide, 7210 SAS-X, R6, R12 Services guide). The counter-mode can be set to either “in-out-profile-count” or “forward-drop-count”.

The statistics collected for the following accounting records listed below vary based on the counter-mode selected:

- 1.Service-ingress-octets
- 2.Service-ingress-packets
- 3.Combined-service-ingress
- 4.Complete-service-ingress-egress

[Table 29](#) and [Table 30](#) depict the changes in the records based on the counter-mode selected.

[Table 29](#) lists the accounting policy record names and the statistics that are collected with each (for 7210 SAS-M in access-uplink mode and network mode).

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
Service-ingress-octets (counter mode is "in-out-profile-count)	sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctetsForwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
ioo	IngressOctetsOffered			
Service-ingress-octets (counter mode is forward-drop-count)	sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		of	OctetsForwarded	
		od	OctetsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
ioo	IngressOctetsOffered			
Service-egress-octets NOTE: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	seo	(Per SAP)	(Per SAP)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
Service-ingress-packets:(counter mode is in-out-profile-count)	sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		ipf	InProfilePktsForwarded	
		opf	OutOfProfilePktsForwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
Service-ingress-packets packets (counter mode is forward-drop-count)	sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		pf	PacketsForwarded	
		pd	PacketsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
Service-egress-packets. NOTE: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	sep	(Per SAP)	(Per SAP)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		pf	PktsForwarded	
		pd	PktsDropped	

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
Combined-service-ingress (counter mode is in-out-profile-count)	sio , sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctetsForwarded	
		ipf	InProfilePktsForwarded	
		opf	OutOfProfilePktsForwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	Access Uplink Network
		sap	SapId	
		ioo	IngressOctetsOffered	
		ipo	IngressPktsOffered	
Combined-service-ingress (counter mode is forward-drop-count)	sio, sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		pf	PacketsForwarded	
		pd	PacketsDropped	
		of	OctetsForwarded	
		od	OctetsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
		ipo	IngressPktsOffered	
Combined-service-egress NOTE: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	seo , sep	(Per SAP)	(Per SAP)	Access Uplink Network

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
		pf	PktsForwarded	
		pd	PktsDropped	
Complete-service-ingress-egress (counter mode is in-out-profile-count) NOTE: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	sio , sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctetsForwarded	
		ipf	InProfilePktsForwarded	
	opf	OutOfProfilePktsForwarded		
	seo , sep	(Per Sap)	(Per Sap)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
		ipo	IngressPktsOffered	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
		od	OctetsDropped	
		pf	PktsForwarded	
		pd	PktsDropped	
Complete-service-ingress-egress (counter mode is forward-drop-count)	sip, sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		pf	PacketsForwarded	
		pd	PacketsDropped	
		of	OctetsForwarded	
		od	OctetsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
		ioo	IngressOctetsOffered	
	seo, sep	(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
pf	PktsForwarded			

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
		pd	PktsDropped	
Access-egress-octets	aeo	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	Octets Dropped	
Access-egress-packets	aep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		pf	PktsForwarded	
		pd	PktsDropped	
Combined-access-egress	cmAeo , cmAep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		pf	PktsForwarded	Access Uplink Network
		pd	PktsDropped	
		od	Octets Dropped	
Network-ingress-octets	nio	(Per Meter)	(Per Meter)	Access Uplink Network
		port	PortId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
Network-ingress-packets	nip	(Per Meter)	(Per Meter)	Access Uplink Network
		port	PortId	
		mId	MeterId	
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Network-egress-octets	neo	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	Octets Dropped	
Network-egress-packets	nep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		pf	PktsForwarded	
		pd	PktsDropped	
Combined-network-egress	cmNeo , cmNep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		pf	PktsForwarded	
		pd	PktsDropped	
		od	OctetsDropped	
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)	Access Uplink Network

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
		port	PortId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
		(Per Queue)	(Per Queue)	
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	OctetsDropped	
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes	
		ipf	InProfilePktsForwarded		
		opf	OutProfilePktsForwarded		
Combined-sdp-ingress-egress	cmSdpipoo,cmSdpepo cmSdpipoo (Ingress)	svc	SvcID	Network	
		sdp	SdpID		
		tpf	TotalPacketsForwarded		
		tof	TotalOctetsForwarded		
	cmSdpepo (Egress)	svc	SvcID		
		sdp	SdpID		
		tpf	TotalPacketsForwarded		
		tof	TotalOctetsForwarded		
Complete-sdp-ingress-egress	cmSdpipoo,cmSdpepo,cpSdpipoo,cpSdpepo			Network	
		cmSdpipoo (Ingress)	svc	SvcID	
			sdp	SdpID	
			tpf	TotalPacketsForwarded	
	tof		TotalOctetsForwarded		
	cmSdpepo (Egress)	svc	SvcID		
		sdp	SdpID		
		tpf	TotalPacketsForwarded		
		tof	TotalOctetsForwarded		
	cpSdpipoo (Ingress)	sdp	SdpID		
		tpf	TotalPacketsForwarded		
		tof	TotalOctetsForwarded		

Table 29: Accounting Record Name Details (for 7210 SAS-M and 7210 SAS-T in access-uplink and network mode) (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	Supported Modes
	cpSdpepo (Egress)	sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	

Table 30 lists the accounting policy record names and the statistics that are collected with each (for 7210 SAS-X)

Table 30: Accounting Record Name Details for 7210 SAS-X

Record Name	Sub Records	Sub Record Fields	Field Description	
Service-ingress-octets(counter mode is in-out-profile-count)	sio	(Per Meter)	(Per Meter)	
		svc	SvcId	SvcId
		sap	SapId	SapId
		mId	MeterId	MeterId
		iof	InProfileOctetsForwarded	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded	OutOfProfileOctetsForwarded
		(Per Queue)	(Per Queue)	(Per Queue)
		svc	SvcId	SvcId
		sap	SapId	SapId
		qId	QueueID	QueueID
		of	OctetsForwarded	OctetsForwarded
		iod	In-profileOctetsDropped	In-profileOctetsDropped
		ood	Out-of-profileOctetsDropped	Out-of-profileOctetsDropped
		(Per SAP)	(Per SAP)	(Per SAP)
		svc	SvcId	SvcId
		sap	SapId	SapId
		ioo	IngressOctetsOffered	IngressOctetsOffered

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Service-ingress-octets (counter mode is forward-drop-count)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		(Per Queue)	(Per Queue)
		qid	Queue-ID
		of	Octets forwarded
		iod	In-profileOctetsDropped
		ood	Out-of-profileOctetsDropped
Service-egress-octets	seo	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	QueueId
		iod	InProfileOctetsDropped
		ood	OutOfProfileOctetsDropped
		of	OctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Service-ingress-packets: (counter mode is in-out-profile-count)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qId	QueueID
		pf	PktsForwarded
		ipd	In-profilePktsDropped
		opd	Out-of-profilePktsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
ipo	IngressPktsOffered		
Service-ingress-packets (counter mode is forward-drop-count)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PktsForwarded
		pd	PktsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPktsOffered
		(Per Queue)	(Per Queue)
		qid	Queue-ID
		pf	Pktsforwarded
		ipd	In-profilePktsDropped
		opd	Out-of-profilePktsDropped

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Service-egress-packets:	sep	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	QueueId
		ipd	InProfilePktsDropped
		opd	OutOfProfilePktsDropped
		pf	PktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPktsForwarded
Combined-service-ingress (counter mode is in-out-profile-count)	sio , sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per Queue)	(Per Queue)
		svc	SvcID
		sap	SapID
		qId	QueueID
		of	OctetsForwarded
		iod	In-profileOctetsDropped
		ood	Out-of-profileOctetsDropped
		pf	PktsForwarded
		ipd	In-profilePktsDropped
		opd	Out-of-profilePktsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
ioo	IngressOctetsOffered		
ipo	IngressPktsOffered		
Combined-service-egress	seo , sep	(Per Queue)	(Per Queue)

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		svc	SvcId
		sap	SapId
		qid	QueueId
		ipd	InProfilePktsDropped
		opd	OutOfProfilePktsDropped
		iod	InProfileOctetsDropped
		ood	OutOfProfileOctetsDropped
		pf	PktsForwarded
		of	OctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Combined-service-ingress(counter mode is forward-drop-count)	sip, sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PktsForwarded
		pd	PktsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per Queue)	(Per Queue)
		svc	SvcID
		sap	SapID
		qId	QueueID
		of	OctetsForwarded
		iod	In-profileOctetsDropped
		ood	Out-of-profileOctetsDropped
		pf	PktsForwarded
		ipd	In-profilePktsDropped
		opd	Out-of-profilePktsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPktsOffered
		ioo	IngressOctetsOffered

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Complete-service-ingress-egress (counter mode is in-out-profile-count)	sio , sip seo , sep	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per Ingress Queue)	(Per Ingress Queue)
		svc	SvcID
		sap	SapID
		qId	QueueID
		of	IngressOctetsForwarded
		iod	IngressIn-profileOctetsDropped
		ood	IngressOut-of-profileOctetsDropped
		pf	IngressPktsForwarded
		ipd	IngressIn-profilePktsDropped
		opd	IngressOut-of-profilePktsDropped
		(Per Sap)	(Per Sap)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
		(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	QueueId
		ipd	InProfilePktsDropped
		pf	PktsForwarded
		opd	OutOfProfilePktsDropped
		iod	InProfileOctetsDropped
ood	OutOfProfileOctetsDropped		
of	OctetsForwarded		

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Complete-service-ingress-egress(counter mode is forward-drop-count)	sip, sio seo, sep	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PktsForwarded
		pd	PktsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per Ingress Queue)	(Per Ingress Queue)
		svc	SvcID
		sap	SapID
		qId	QueueID
		of	IngressOctetsForwarded
		iod	IngressIn-profileOctetsDropped
		ood	IngressOut-of-profileOctetsDropped
		pf	IngressPktsForwarded
		ipd	IngressIn-profilePktsDropped
		opd	IngressOut-of-profilePktsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPktsOffered
		ioo	IngressOctetsOffered
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
		(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	QueueId
		ipd	InProfilePktsDropped
		pf	PktsForwarded
		opd	OutOfProfilePktsDropped
		iod	InProfileOctetsDropped
ood	OutOfProfileOctetsDropped		
of	OctetsForwarded		
Network-ingress-octets	nio	(Per Meter)	
		port	PortId

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-ingress-packets	nip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Network-egress-octets	neo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Network-egress-packets	nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-network-egress	cmNeo , cmNep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		od	OctetsDropped
Combined-network-egress	cmNio,cmNep	pd	PktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Network-interface- ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iofIn	ProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
Network-interface- ingress- packets	niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		ipfIn	ProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
Combined-network- interface-ingress	niio, niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iofIn	ProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipfIn	ProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
Combined-sdp- ingress-egress	cmSdpipo,cm Sdpepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPktsForwarded
		tof	TotalOctetsForwarded
Complete-sdp- ingress-egress	cmSdpipo,cm Sdpepo,cpSdp ipo,cpSdpepo		

Table 30: Accounting Record Name Details for 7210 SAS-X (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
	cmSdpipo (Ingress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPktsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPktsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo (Ingress)	sdp	SdpID
		tpf	TotalPktsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo (Egress)	sdp	SdpID
tpf		TotalPktsForwarded	
tof		TotalOctetsForwarded	

Table 31 lists the accounting policy record names and the statistics for 7210 SAS-R6 and 7210 SAS-R12.

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12

Record Name	Sub Records	Sub Record Fields	Field Description
Service-ingress-octets (counter mode is "in-out-profilecount")	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-ingress-octets (counter mode is forward-drop-count)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		of	OctetsForwarded
		od	OctetsDropped
Service-ingress-packets:(counter mode is in-out-profile-count)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPacketsOffered
Service-ingress-packets packets (counter mode is forward-drop-count)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		sap	SapId
		ipo	IngressPacketsOffered
Service-egress-packets NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	sep	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		pf	PacketsForwarded
		pd	PacketsDropped
Combined-service-ingress (counter mode is in-out-profile-count)	sio , sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Combined-service-ingress (counter mode is forward-drop-count)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-egress NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		of	OctetsForwarded
od	OctetsDropped		
pf	PacketsForwarded		
pd	PacketsDropped		

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Complete-service-ingress-egress (counter mode is in-out-profile-count) NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	sio , sip	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
	seo , sep	(Per Sap)	(Per Sap)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
	seo sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
	of	OctetsForwarded	
	od	OctetsDropped	
	pf	PacketsForwarded	
	pd	PacketsDropped	

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
<p>Complete-service-ingress-egress (counter mode is forward-drop-count)</p> <p>NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.</p>	sip, sio	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
		seo, sep	(Per Egress Queue)
	svc		SvcId
	sap		SapId
	qid		EgressQueueId
	of		OctetsForwarded
	od		OctetsDropped
	pf		PacketsForwarded
	pd		PacketsDropped
	(Per SAP)		(Per SAP)
	svc		SvcId
	sap		SapId
	eof		EgressOctetsForwarded
	epf		EgressPktsForwarded
	(Per SAP Egress Meter)		(Per SAP Egress Meter)
	mId	Egress Meter ID	
of	OctetsForwarded		
od	OctetsDropped		
pf	PacketsForwarded		
pd	PacketsDropped		

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Access-egress-octets NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	a eo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Access-egress-packets NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	a ep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-access-egress NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	cmAeo , cmAep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
Network-ingress-octets	nio	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-ingress-packets	nip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Network-egress-octets	neo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Network-egress-packets	nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-network-egress	cmNeo , cmNep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
		od	OctetsDropped
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded

Table 31: Accounting Record Name Details for 7210 SAS-R6 and 7210 SAS-R12 (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description	
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)	
		NwIf	IpInterface	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Combined-sdp-ingress-egress	cmSdpipo,c mSdpepo cmSdpipo (Ingress)			
		svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
	tof	TotalOctetsForwarded		
Complete-sdp-ingress-egress	cmSdpipo,c mSdpepo,cp Sdpipo,cpSd pepo			
		cmSdpipo (Ingress)	svc	SvcID
			sdp	SdpID
	tpf		TotalPacketsForwarded	
	tof		TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cpSdpipo (Ingress)	sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cpSdpepo (Egress)	sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	

Table 32 lists the accounting policy record names and the statistics for 7210 SAS-Mxp

Table 32: Accounting Record Name Details for 7210 SAS-Mxp

Record Name	Sub Records	Sub Record Fields	Field Description
Service-ingress-octets (counter mode is "in-out-profilecount")	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-ingress-octets (counter mode is forward-drop-count)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
Service-ingress-packets:(counter mode is in-out-profile-count)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description		
		(Per SAP)	(Per SAP)		
		svc	SvcId		
		sap	SapId		
		ipo	IngressPacketsOffered		
Service-ingress-packets packets (counter mode is forward-drop-count)	sip	(Per Meter)	(Per Meter)		
		svc	SvcId		
		sap	SapId		
		mId	MeterId		
		pf	PacketsForwarded		
		pd	PacketsDropped		
		(Per SAP)	(Per SAP)		
		svc	SvcId		
		sap	SapId		
		ipo	IngressPacketsOffered		
Service-egress-packets NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sep	(Per Egress queue)	(Per Egress queue)		
		svc	SvcId		
		sap	SapId		
		qid	Egress QueueId		
		pf	PacketsForwarded		
		pd	PacketsDropped		
		(Per SAP)	(Per SAP)		
		svc	SvcId		
		sap	SapId		
				epf	EgressPktsForwarded
Combined-service-ingress (counter mode is in-out-profile-count)	sio , sip	(Per Meter)	(Per Meter)		
		svc	SvcId		
		sap	SapId		
		mId	MeterId		
		iof	InProfileOctetsForwarded		
		oof	OutOfProfileOctetsForwarded		
		ipf	InProfilePktsForwarded		
		opf	OutOfProfilePktsForwarded		
		(Per SAP)	(Per SAP)		
		svc	SvcId		
		sap	SapId		
				ioo	IngressOctetsOffered
				ipo	IngressPacketsOffered

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Combined-service-ingress (counter mode is forward-drop-count)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-egress NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Complete-service-ingress-egress (counter mode is in-out-profile-count) NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sio , sip	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
	seo , sep	(Per Sap)	(Per Sap)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
	seo sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
eof		EgressOctetsForwarded	
epf	EgressPacketsForwarded		
Complete-service-ingress-egress (counter mode is forward-drop-count) NOTE: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sip, sio	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		ipo	IngressPacketsOffered
	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
	epf	EgressPktsForwarded	
Access-egress-octets NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	aeo	(Per Queue)	(Per Queue)
	port	PortId	
	qId	QueueId	
	of	OctetsForwarded	
	od	Octets Dropped	
Access-egress-packets NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	aep	(Per Queue)	(Per Queue)
	port	PortId	
	qId	QueueId	
	pf	PktsForwarded	
	pd	PktsDropped	
Combined-access-egress NOTE: This accounting record is applicable only when port-based queuing and scheduling is used. It is not available in SAP based queuing and scheduling.	cmAeo , cmAep	(Per Queue)	(Per Queue)
	port	PortId	
	qId	QueueId	
	of	OctetsForwarded	
	pf	PktsForwarded	
	pd	PktsDropped	
	od	Octets Dropped	
Network-ingress-octets	nio	(Per Meter)	(Per Meter)
	port	PortId	
	mId	MeterId	
	iof	InProfileOctetsForwarded	
	oof	OutProfileOctetsForwarded	

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
Network-ingress-packets	nip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Network-egress-octets	neo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Network-egress-packets	nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-network-egress	cmNeo , cmNep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)

Table 32: Accounting Record Name Details for 7210 SAS-Mxp (Continued)

Record Name	Sub Records	Sub Record Fields	Field Description
		NwIf	IpInterface
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-sdp-ingress-egress	cmSdpipo,c mSdpepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
	tof	TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
tof		TotalOctetsForwarded	
Complete-sdp-ingress-egress	cmSdpipo,c mSdpepo,cp Sdpipo,cpSd pepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
	tof	TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo (Ingress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo (Egress)	sdp	SdpID
		tpf	TotalPacketsForwarded
tof		TotalOctetsForwarded	

Configuration Guidelines

Before modifying the counter, disable account log generation. Execute the `no collect-stats` command. Changing the mode of the counter results in loss of previously collected counts and resets the counter.

Accounting Files

When a policy has been created and applied to a service or network port, the accounting file is stored on the compact flash in a compressed XML file format. The device creates two directories on the compact flash to store the files. The following output displays a directory named act-collect that holds accounting files that are open and actively collecting statistics. The directory named act stores the files that have been closed and are awaiting retrieval.

```
ALA-1>file cfl:\# dir act*
12/19/2006 06:08a <DIR> act-collect
12/19/2006 06:08a <DIR> act

ALA-1>file cfl:\act-collect\ # dir
Directory of cfl:\act-collect#
12/23/2006 01:46a <DIR> .
12/23/2006 12:47a <DIR> ..
12/23/2006 01:46a 112 act1111-20031223-014658.xml.gz
12/23/2006 01:38a 197 act1212-20031223-013800.xml.gz
```

Accounting files always have the prefix act followed by the accounting policy ID, log ID and timestamp. The accounting log file naming and log file destination properties like rollover and retention are discussed in more detail in [Log Files on page 215](#).

Design Considerations

When preparing for an accounting policy deployment, verify that data collection, file rollover, and file retention intervals are properly tuned for the amount of statistics to be collected.

If the accounting policy collection interval is too brief, there may be insufficient time to store the data from all the services within the specified interval. If that is the case, some records may be lost or incomplete. Interval time, record types, and number of services using an accounting policy are all factors that should be considered when implementing accounting policies.

The rollover and retention intervals on the log files and the frequency of file retrieval must also be considered when designing accounting policy deployments. The amount of data stored depends on the type of record collected, the number of services that are collecting statistics, and the collection interval that is used.

Configuration Notes

This section describes logging configuration caveats.

- A file or filter cannot be deleted if it has been applied to a log.
- File IDs, syslog IDs, or SNMP trap groups must be configured before they can be applied to a log ID.
- A file ID can only be assigned to *either* one log ID *or* one accounting policy.
- Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.
- The **snmp-trap-id** must be the same as the **log-id**.

Configuring Logging with CLI

This section provides information to configure logging using the command line interface.

Topics in this section include:

- [Log Configuration Overview on page 272](#)
→ [Log Types on page 272](#)
- [Basic Event Log Configuration on page 273](#)
- [Common Configuration Tasks on page 274](#)
- [Log Management Tasks on page 283](#)

Log Configuration Overview

Configure logging parameters to save information in a log file or direct the messages to other devices. Logging does the following:

- Provides you with logging information for monitoring and troubleshooting.
 - Allows you to select the types of logging information to be recorded.
 - Allows you to assign a severity to the log messages.
 - Allows you to select the source and target of logging information.
-

Log Types

Logs can be configured in the following contexts:

- **Log file** — Log files can contain log event message streams or accounting/billing information. Log file IDs are used to direct events, alarms/traps and debug information to their respective targets.
- **SNMP trap groups** — SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.
- **Syslog** — Information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element.
- **Event control** — Configures a particular event or all events associated with an application to be generated or suppressed.
- **Event filters** — An event filter defines whether to forward or drop an event or trap based on match criteria.
- **Accounting policies** — An accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more s access object or network objects.
- **Event logs** — An event log defines the types of events to be delivered to its associated destination.
- **Event throttling rate** — Defines the rate of throttling events.

Basic Event Log Configuration

The most basic log configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays a log configuration example.

```
A:ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
    event-control 2001 generate critical
    file-id 1
        description "This is a test file-id."
        location cf1:
    exit
    file-id 2
        description "This is a test log."
        location cf1:
    exit
    snmp-trap-group 7
        trap-target 11.22.33.44 "snmpv2c" notify-community "public"
    exit
    log-id 2
        from main
        to file 2
    exit
-----
A:ALA-12>config>log#
```

Common Configuration Tasks

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

- [Configuring a File ID on page 276](#)
 - [Configuring an Event Log on page 274](#)
 - [Configuring an Accounting Policy on page 277](#)
 - [Configuring Event Control on page 278](#)
 - [Configuring a Log Filter on page 280](#)
 - [Configuring an SNMP Trap Group on page 281](#)
 - [Configuring a Syslog Target on page 282](#)
-

Configuring an Event Log

An event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

```
CLI Syntax: config>log
                log-id log-id
                description description-string
                filter filter-id
                from {[main] [security] [change] [debug-trace]}
                to console
                to file file-id
                to memory [size]
                to session
                to snmp [size]
                to syslog syslog-id}
                time-format {local|utc}
                no shutdown
```

The following displays a log file configuration example:

```
ALA-12>config>log>log-id# info
-----
...
  log-id 2
    description "This is a test log file."
    filter 1
    from main security
    to file 1
  exit
...
-----
ALA-12>config>log>log-id#
```

Configuring a File ID

To create a log file, a file ID is defined, the target CF or USB drive is specified, and the rollover ,retention interval period for the log file is defined. The rollover interval is defined in minutes and determines how long a file will be used before it is closed and a new log file is created. The retention interval determines how long the file will be stored on the storage device before it is deleted.

Use the following CLI syntax to configure a log file:

CLI Syntax: config>log
file-id *log-file-id*
description *description-string*
location *cflash-id*
rollover *minutes* [*retention hours*]

CLI Syntax: For 7210 SAS-T
config>log
file-id *log-file-id*
description *description-string*
location *cflash/usb-flash-id [backup-cflash-id]*
rollover *minutes* [*retention hours*]

The following displays a log file configuration example:

```
A:ALA-12>config>log# info
-----
file-id 1
description "This is a log file."
location cf1:
rollover 600 retention 24
exit
-----
A:ALA-12>config>log#
```

Configuring an Accounting Policy

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory or compact flash (cf1:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See [Configuring an Event Log on page 274](#) and [Configuring a File ID on page 276](#).

Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one access, one access port, one network, one network interface and one SDP accounting policy can be defined as default. If statistics collection is enabled on an accounting object, and no accounting policy is applied, then the respective default accounting policy is used. If no default policy is defined, then no statistics are collected unless a specifically-defined accounting policy is applied.

Use the following CLI syntax to configure an accounting policy:

CLI Syntax:

```
config>log>
  accounting-policy acct-policy-id interval minutes
  description description-string
  default
  record record-name
  to file log-file-id
  no shutdown
```

The following displays a accounting policy configuration example:

```
A:ALA-12>config>log# info
-----
  accounting-policy 5
  description "This is a test accounting policy."
  record service-ingress-packets
  to file 3
  exit
-----
A:ALA-12>config>log#
```

Configuring Event Control

Use the following CLI syntax to configure event control. Note that the **throttle** parameter used in the **event-control** command syntax enables throttling for a specific event type. The **config>log>throttle-rate** command configures the number of events and interval length to be applied to all event types that have throttling enabled by this **event-control** command.

CLI Syntax:

```
config>log
    event-control application-id [event-name|event-number] generate [severity-level] [throttle]
    event-control application-id [event-name|event-number] suppress
    throttle-rate events [interval seconds]
```

The following displays an event control configuration:

```
A:ALA-12>config>log# info
#-----
echo "Log Configuration"
#-----
    throttle-rate 500 interval 10
    event-control "oam" 2001 generate throttle
    event-control "ospf" 2001 suppress
    event-control "ospf" 2003 generate cleared
    event-control "ospf" 2014 generate critical
..
#-----
A:ALA-12>config>log>filter#
```

Configuring Throttle Rate

This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the **event-control** command.

Use the following CLI syntax to configure the throttle rate.

CLI Syntax: `config>log#
throttle-rate events [interval seconds]`

The following displays a throttle rate configuration example:

```
*A:gall171>config>log# info
-----
throttle-rate 500 interval 10
event-control "aps" 2001 generate throttle
-----
*A:gall171>config>log#
```

Configuring a Log Filter

Use the following CLI syntax to configure a log filter:

```

CLI Syntax: config>log
                filter filter-id
                  default-action {drop|forward}
                  description description-string
                  entry entry-id
                    action {drop|forward}
                    description description-string
                    match
                      application {eq|neq} application-id
                      number {eq|neq|lt|lte|gt|gte} event-id
                      router {eq|neq} router-instance [regex]
                      severity {eq|neq|lt|lte|gt|gte} severity-level
                      subject {eq|neq} subject [regex]

```

The following displays a log filter configuration example:

```

A:ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
    file-id 1
      description "This is our log file."
      location cfl:
      rollover 600 retention 24
    exit
    filter 1
      default-action drop
      description "This is a sample filter."
      entry 1
        action forward
        match
          application eq "mirror"
          severity eq critical
        exit
      exit
    exit
...
    log-id 2
      shutdown
      description "This is a test log file."
      filter 1
      from main security
      to file 1
    exit
...
#-----
A:ALA-12>config>log#

```

Configuring an SNMP Trap Group

The associated *log-id* does not have to be configured before a **snmp-trap-group** can be created, however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

Use the following CLI syntax to configure an SNMP trap group:

```
CLI Syntax:  config>log
                snmp-trap-group log-id
                  trap-target name [address ip-address] [port port]
                    [snmpv1|snmpv2c| snmpv3] notify-community communi-
                    tyName |snmpv3SecurityName [security-level {no-
                    auth-no-privacy|auth-no-privacy|privacy}]
```

The following displays a basic SNMP trap group configuration example:

```
A:ALA-12>config>log# info
-----
...
    snmp-trap-group 2
      trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
      exit
...
    log-id 2
      description "This is a test log file."
      filter 1
      from main security
      to file 1
    exit
...
-----
A:ALA-12>config>log#
```

Configuring a Syslog Target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

Use the following CLI syntax to configure a syslog file:

CLI Syntax: `config>log`
`syslog syslog-id`
`description description-string`
`address ip-address`
`log-prefix log-prefix-string`
`port port`
`level {emergency|alert|critical|error|warning|notice|info|debug}`
`facility syslog-facility`

The following displays a syslog configuration example:

```
A:ALA-12>config>log# info
-----
...
    syslog 1
      description "This is a syslog file."
      address 10.10.10.104
      facility user
      level warning
    exit
...
-----
A:ALA-12>config>log#
```

Log Management Tasks

This section discusses the following logging tasks:

- [Modifying a Log File on page 284](#)
- [Deleting a Log File on page 286](#)
- [Modifying a File ID on page 287](#)
- [Deleting a File ID on page 289](#)
- [Modifying a Syslog ID on page 290](#)
- [Deleting a Syslog on page 291](#)
- [Modifying an SNMP Trap Group on page 292](#)
- [Deleting an SNMP Trap Group on page 293](#)
- [Modifying a Log Filter on page 294](#)
- [Deleting a Log Filter on page 296](#)
- [Modifying Event Control Parameters on page 297](#)
- [Returning to the Default Event Control Configuration on page 298](#)

Modifying a Log File

Use the following CLI syntax to modify a log file:

```
CLI Syntax: config>log
                log-id log-id
                  description description-string
                  filter filter-id
                  from {[main] [security] [change] [debug-trace]}
                  to console
                  to file file-id
                  to memory [size]
                  to session
                  to snmp [size]
                  to syslog syslog-id}
```

The following displays the current log configuration:

```
ALA-12>config>log>log-id# info
-----
...
  log-id 2
    description "This is a test log file."
    filter 1
    from main security
    to file 1
  exit
...
-----
ALA-12>config>log>log-id#
```

The following displays an example to modify log file parameters:

```
Example: config# log
            config>log# log-id 2
            config>log>log-id# description "Chassis log file."
            config>log>log-id# filter 2
            config>log>log-id# from security
            config>log>log-id# exit
```

The following displays the modified log file configuration:

```
A:ALA-12>config>log# info
-----
...
  log-id 2
      description "Chassis log file."
      filter 2
      from security
      to file 1
  exit
...
-----
A:ALA-12>config>log#
```

Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, **file 1** is associated with **log-id 2**.

```
A:ALA-12>config>log# info
-----
file-id 1
  description "LocationTest."
  location cfl:
  rollover 600 retention 24
  exit
...
log-id 2
  description "Chassis log file."
  filter 2
  from security
  to file 1
  exit
...
-----
A:ALA-12>config>log#
```

Use the following CLI syntax to delete a log file:

CLI Syntax:

```
config>log
  no log-id log-id
  shutdown
```

The following displays an example to delete a log file:

Example:

```
config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

Modifying a File ID

NOTE: When the **file-id** location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear>log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log not cleared, the old location remains in effect.

The location can be CF (cflash-id) or USB(usb-flash-id).

Use the following CLI syntax to modify a log file:

CLI Syntax:

```
config>log
  file-id log-file-id
  description description-string
  location [cflash-id]
  rollover minutes [retention hours]
```

The following displays the current log configuration:

```
A:ALA-12>config>log# info
-----
  file-id 1
    description "This is a log file."
    location cfl:
    rollover 600 retention 24
  exit
-----
A:ALA-12>config>log#
```

The following displays an example to modify log file parameters:

Example:

```
config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file modifications:

```
A:ALA-12>config>log# info
-----
...
  file-id 1
    description "LocationTest."
    location cfl:
    rollover 2880 retention 500
  exit
...
-----
```

Log Management Tasks

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

Deleting a File ID

NOTE: All references to the file ID must be deleted before the file ID can be removed.

Use the following CLI syntax to delete a log ID:

CLI Syntax: `config>log`
`no file-id log-file-id`

The following displays an example to delete a file ID:

Example: `config>log# no file-id 1`

Modifying a Syslog ID

NOTE: All references to the syslog ID must be deleted before the syslog ID can be removed.

Use the following CLI syntax to modify a syslog ID parameters:

CLI Syntax:

```
config>log
  syslog syslog-id
        description description-string
        address ip-address
        log-prefix log-prefix-string
        port port
        level {emergency|alert|critical|error|warning|notice|info|debug}
        facility syslog-facility
```

The following displays an example of the syslog ID modifications:

Example:

```
config# log
config>log# syslog 1
config>log>syslog$ description "Test syslog."
config>log>syslog# address 10.10.0.91
config>log>syslog# facility mail
config>log>syslog# level info
```

The following displays the syslog configuration:

```
A:ALA-12>config>log# info
-----
...
  syslog 1
    description "Test syslog."
    address 10.10.10.91
    facility mail
    level info
  exit
...
-----
A:ALA-12>config>log#
```

Deleting a Syslog

Use the following CLI syntax to delete a syslog file:

CLI Syntax: `config>log`
`no syslog syslog-id`

The following displays an example to delete a syslog ID:

Example: `config# log`
`config>log# no syslog 1`

Modifying an SNMP Trap Group

Use the following CLI syntax to modify an SNMP trap group:

CLI Syntax: `config>log`
 `snmp-trap-group log-id`
 `trap-target name [address ip-address] [port port]`
 `[snmpv1|snmpv2c| snmpv3] notify-community communi-`
 `tyName |snmpv3SecurityName [security-level {no-`
 `auth-no-privacy|auth-no-privacy|privacy}]`

The following displays the current SNMP trap group configuration:

```
A:ALA-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
        exit
...
-----
A:ALA-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

Example: `config# log`
 `config>log# snmp-trap-group 10`
 `config>log>snmp-trap-group# no trap-target 10.10.10.104:5`
 `config>log>snmp-trap-group# snmp-trap-group# trap-target`
 `10.10.0.91:1 snmpv2c notify-community "com1"`

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
        exit
...
-----
A:ALA-12>config>log#
```

Deleting an SNMP Trap Group

Use the following CLI syntax to delete a trap target and SNMP trap group:

CLI Syntax: `config>log`
 `no snmp-trap-group log-id`
 `no trap-target name`

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
    exit
...
-----
A:ALA-12>config>log#
```

The following displays an example to delete a trap target and an SNMP trap group.

Example: `config>log# snmp-trap-group 10`
 `config>log>snmp-trap-group# no trap-target 10.10.0.91:1`
 `config>log>snmp-trap-group# exit`
 `config>log# no snmp-trap-group 10`

Modifying a Log Filter

Use the following CLI syntax to modify a log filter:

```
CLI Syntax: config>log
                filter filter-id
                  default-action {drop|forward}
                  description description-string
                  entry entry-id
                    action {drop|forward}
                    description description-string
                    match
                      application {eq|neq} application-id
                      number {eq|neq|lt|lte|gt|gte} event-id
                      router {eq|neq} router-instance [regex]
                      severity {eq|neq|lt|lte|gt|gte} severity-level
                      subject {eq|neq} subject [regex]
```

The following output displays the current log filter configuration:

```
ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
...
    filter 1
      default-action drop
      description "This is a sample filter."
      entry 1
        action forward
        match
          application eq "mirror"
          severity eq critical
        exit
      exit
    exit
  ...
#-----
ALA-12>config>log#
```

The following displays an example of the log filter modifications:

```
Example: config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
```

```
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
A:ALA-12>config>log>filter# info
-----
...
    filter 1
      description "This allows <n>."
      entry 1
        action drop
        match
          application eq "user"
          number eq 2001
        exit
      exit
    exit
...
-----
A:ALA-12>config>log>filter#
```

Deleting a Log Filter

Use the following CLI syntax to delete a log filter:

CLI Syntax: `config>log
no filter filter-id`

The following output displays the current log filter configuration:

```
A:ALA-12>config>log>filter# info
-----
...
    filter 1
      description "This allows <n>."
      entry 1
        action drop
        match
          application eq "user"
          number eq 2001
        exit
      exit
    exit
...
-----
A:ALA-12>config>log>filter#
```

The following displays an example of the command usage to delete a log filter:

Example: `config>log# no filter 1`

Modifying Event Control Parameters

Use the following CLI syntax to modify event control parameters:

CLI Syntax: `config>log`
 `event-control application-id [event-name|event-number] generate[severity-level] [throttle]`
 `event-control application-id [event-name|event-number] suppress`

The following displays the current event control configuration:

```
A:ALA-12>config>log# info
-----
...
    event-control 2014 generate critical
...
-----
A:ALA-12>config>log#
```

The following displays an example of an event control modifications:

Example: `config# log`
 `config>log# event-control 2014 suppress`

The following displays the log filter configuration:

```
A:ALA-12>config>log# info
-----
...
    event-control 2014 suppress
...
-----
A:ALA-12>config>log#
```

Returning to the Default Event Control Configuration

The **no** form of the **event-control** command returns modified values back to the default values.

Use the following CLI syntax to modify event control parameters:

CLI Syntax: `config>log`
`no event-control application [event-name |event-number]`

The following displays an example of the command usage to return to the default values:

Example: `config# log`
`config>log# no event-control 2001`
`config>log# no event-control 2002`
`config>log# no event-control 2014`

```
A:ALA-12>config>log# info detail
-----
#-----
echo "Log Configuration"
#-----
      event-control 2001 generate minor
      event-control 2002 generate warning
      event-control 2003 generate warning
      event-control 2004 generate critical
      event-control 2005 generate warning
      event-control 2006 generate warning
      event-control 2007 generate warning
      event-control 2008 generate warning
      event-control 2009 generate warning
      event-control 2010 generate warning
      event-control 2011 generate warning
      event-control 2012 generate warning
      event-control 2013 generate warning
      event-control 2014 generate warning
      event-control 2015 generate critical
      event-control 2016 generate warning
...
-----
A:ALA-12>config>log#
```

Configuring SNMP Dying Gasp

NOTE: SNMP dying gasp (IPv4) is not supported on 7210 SAS-R6 and 7210 SAS-12 devices, but supported on all other 7210 SAS devices. SNMP dying gasp (IPv6) is not supported on any of the 7210 SAS devices.

Use the following CLI syntax to configure SNMP dying gasp:

CLI Syntax: config>log
 no snmp-dying-gasp primary <trap-target-group-num> < trap-target-
 name> [secondary {<trap-target-group-num><trap-target-name>}
 [tertiary {<trap-target-group-num> <trap-target- name>}]]

Sample Configuration

```
*A:Dut-A>config>log# snmp-dying-gasp primary 7 server1 secondary 8 server2
*A:Dut-A>config>log# info
-----
      snmp-trap-group 7
        trap-target "server1" address 1.1.1.1 snmpv2c notify-community "public"
      exit
      snmp-trap-group 8
        trap-target "server2" address 10.135.2.10 snmpv3 notify-community "snmpv3user"
security-level auth-no-privacy
      exit
      snmp-trap-group 9
        trap-target "server3" address 2.2.2.2 snmpv3 notify-community "snmpv3user"
security-level auth-no-privacy
      exit
      log-id 7
        from main
        to snmp
      exit
      log-id 8
        from main
        to snmp
      exit
      log-id 9
        from main
        to snmp
      exit
      snmp-dying-gasp primary 7 "server1" secondary 8 "server2"
-----
*A:Dut-A>config>log#
```

Configuration Guidelines for SNMP Dying Gasp Trap

The system does not try to resolve the ARP when it needs to send out the SNMP dying-gasp trap, since the amount of time available during power loss event is very less. Instead, the system assumes that ARP entry to the gateway used to reach the SNMP trap server is always available. It is recommended that user run a periodic ping query to the SNMP trap server in the background using the cron utility.

Sample configuration of a cron job which initiates a ping to the server mentioned in the pingscript file every one minute:

```
*7210-SAS># configure cron
*7210-SAS >config>cron# info
-----
      time-range "NO-TIME-RANGE" create
      description "NO-TIME-RANGE is the default always-on time-range"
      exit
-----
7210SAS>config>cron#
```

Log Command Reference

Command Hierarchies

- [Log Command Reference on page 301](#)
 - [Accounting Policy Commands on page 302](#)
 - [File ID Commands on page 302](#)
 - [Event Filter Commands on page 302](#)
 - [Log ID Commands on page 304](#)
 - [SNMP Trap Group Commands on page 304](#)
 - [Syslog Commands on page 305](#)
- [Show Commands on page 305](#)
- [Clear Command on page 305](#)

Log Configuration Commands

```

config
  — log
    — event-control application-id [event-name | event-number] [generate [severity-level] [throt-
      tle]
    — event-control application-id [event-name | event-number] suppress
    — no event-control application [event-name | event-number]
    — route-preference primary {inband | outband} secondary {inband | outband | none}
    — no route-preference
    — throttle-rate events [interval seconds]
    — no throttle-rate

```

ACCOUNTING POLICY COMMANDS

```
config
  — log
    — accounting-policy acct-policy-id
    — no accounting-policy acct-policy-id
      — [no] default
      — collection-interval minutes
      — [no] collection-interval
      — description description-string
      — no description
      — [no] log-memory
      — record record-name
      — no record
      — [no] shutdown
      — [no] to file log-file-id
```

FILE ID COMMANDS

```
config
  — log
    — [no] file-id log-file-id
      — description description-string
      — no description
      — location [cflash-id | usb-flash-id] [backup-cflash-id]
      — rollover minutes [retention hours]
      — no rollover
```

EVENT FILTER COMMANDS

```
config
  — log
    — [no] filter filter-id
      — default-action {drop | forward}
      — no default-action
      — description description-string
      — no description
      — [no] entry entry-id
        — action {drop | forward}
        — no action
        — description description-string
        — no description
        — [no] match
          — application {eq | neq} application-id
          — no application
          — number {eq | neq | lt | lte | gt | gte} event-id
          — no number
          — router {eq | neq} router-instance [regex]
          — no router
          — severity {eq | neq | lt | lte | gt | gte} severity-level
          — no severity
          — subject {eq | neq} subject [regex]
```

— **no subject**

LOG ID COMMANDS

```

config
  — log
    — [no] log-id log-id
      — description description-string
      — no description
      — filter filter-id
      — no filter
      — from {[main] [security] [change] [debug-trace]}
      — no from
      — [no] shutdown
      — time-format {local | utc}
      — to console
      — to file log-file-id
      — to memory [size]
      — to session
      — to snmp [size]
      — to syslog syslog-id
  
```

SNMP TRAP GROUP COMMANDS

```

config
  — log
    — [no] snmp-trap-group log-id
      — description description-string
      — no description
      — trap-target name [address ip-address] [port port] [snmpv1 | snmpv2c | snmpv3] notify-community communityName | snmpv3SecurityName [security-level {no-auth-no-privacy | auth-no-privacy | privacy}][replay]]
      — no trap-target name
    — [no] snmp-dying-gasp primary trap-target-group-num trap-target-name [secondary {trap-target-group-num trap-target-name} [tertiary {trap-target-group-num trap-target-name}]]]
  
```

SYSLOG COMMANDS

```

config
  — log
    — [no] syslog syslog-id
      — address ip-address
      — no address
      — description description-string
      — no description
      — facility syslog-facility
      — no facility
      — level { emergency | alert | critical | error | warning | notice | info | debug }
      — no level
      — log-prefix log-prefix-string
      — no log-prefix
      — port port
      — no port

```

Show Commands

```

show
  — log
    — accounting-policy [acct-policy-id] [access | network]
    — accounting-records
    — applications
    — event-control [application-id [event-name | event-number]]
    — file-id [log-file-id]
    — filter-id [filter-id]
    — log-collector
    — log-id [log-id] [severity severity-level] [application application] [sequence from-seq [to-seq]] [count count] [router router-instance] [expression]] [subject subject [regexp]] [ascending | descending]
    — snmp-trap-group [log-id]
    — syslog [syslog-id]

```

Clear Command

```

clear
  — log log-id

```

Tools Dump Commands

```

tools
  — dump
    — accounting-policy [id] flash-write-count [clear] (For more information, see 7210 SAS OAM and Diagnostics Guide)

```

Configuration Commands

Generic Commands

description

Syntax	description <i>string</i> no description
Context	config>log>filter config>log>filter>entry config>log>log-id config>log>accounting-policy config>log>file-id config>log>syslog config>log>snmp-trap-group
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 the command removes the string from the configuration.
Default	No text description is associated with this configuration. The string must be entered.
Parameters	<i>string</i> — The description can contain a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>log>log-id config>log>accounting-policy
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.
Default	no shutdown
Special Cases	log-id <i>log-id</i> — When a <i>log-id</i> is shut down, no events are collected for the entity. This leads to the loss of event data.

accounting-policy *accounting Policy* — When an accounting policy is shut down, no accounting data is written to the destination log ID. Counters in the billing data reflect totals, not increments, so when the policy is re-enabled (**no shutdown**) the counters include the data collected during the period the policy was shut down.

Event Control

event-control

Syntax	<p>event-control <i>application-id</i> [<i>event-name</i> <i>event-number</i>] [generate [<i>severity-level</i>] [throttle]</p> <p>event-control <i>application-id</i> [<i>event-name</i> <i>event-number</i>] suppress</p> <p>no event-control <i>application</i> [<i>event-name</i> <i>event-number</i>]</p>
Context	config>log
Description	<p>This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.</p> <p>Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation which directs it to be generated or suppressed.</p> <p>Events are generated with a default severity level that can be modified by using the <i>severity-level</i> option.</p> <p>Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are squelched. In reverse, indiscriminate application may cause excessive overhead.</p> <p>The rate of event generation can be throttled by using the throttle parameter.</p> <p>The no form of the command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, suppress, and throttle options will also be reset to the initial values.</p>
Default	Each event has a set of default settings. To display a list of all events and the current configuration use the event-control command.
Parameters	<p><i>application-id</i> — The application whose events are affected by this event control filter.</p> <p>Default None, this parameter must be explicitly specified.</p> <p>Values A valid application name. To display a list of valid application names, use the applications command. Valid applications are:</p> <p><i>event-name</i> <i>event-number</i> — To generate, suppress, or revert to default for a single event, enter the specific number or event short name. If no event number or name is specified, the command applies to all events in the application. To display a list of all event short names use the event-control command.</p> <p>Default none</p> <p>Values A valid event name or event number.</p>

generate — Specifies that logger event is created when this event occurs. The generate keyword can be used with two optional parameters, *severity-level* and **throttle**.

Default generate

severity-name — An ASCII string representing the severity level to associate with the specified generated events

Default The system assigned severity name

Values One of: cleared, indeterminate, critical, major, minor, warning.

throttle — Specifies whether or not events of this type will be throttled.
By default, event throttling is on for most event types.

suppress — This keyword indicates that the specified events will not be logged. If the **suppress** keyword is not specified then the events are generated by default.

Default generate

route-preference

Syntax	route-preference primary {inband outband} secondary {inband outband none} no route-preference
Context	config>log
Description	<p>This command specifies the primary and secondary routing preference for traffic generated for SNMP notifications and syslog messages. If the remote destination is not reachable through the routing context specified by primary route preference then the secondary routing preference will be attempted.</p> <p>The no form of the command reverts to the default values.</p>
Default	no route-preference
Parameters	<p>primary — Specifies the primary routing preference for traffic generated for SNMP notifications and syslog messages.</p> <p>Default outband</p> <p>secondary — Specifies the secondary routing preference for traffic generated for SNMP notifications and syslog messages. The routing context specified by the secondary route preference will be attempted if the remote destination was not reachable by the primary routing preference, specified by primary route preference. The value specified for the secondary routing preference must be distinct from the value for primary route preference.</p> <p>Default inband</p> <p>inband — Specifies that the logging utility will attempt to use the base routing context to send SNMP notifications and syslog messages to remote destinations.</p> <p>outband — Specifies that the logging utility will attempt to use the management routing context to send SNMP notifications and syslog messages to remote destinations.</p>

none — Specifies that no attempt will be made to send SNMP notifications and syslog messages to remote destinations.

Log File Commands

file-id

Syntax	[no] file-id <i>file-id</i>
Context	config>log
Description	<p>This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.</p> <p>This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the to command under log-id or accounting-policy to direct specific logging or billing source streams to the file destination.</p> <p>A file ID can only be assigned to either <i>one</i> log-id or <i>one</i> accounting-policy. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.</p> <p>A file is created when the file ID defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.</p>

The file names for a log are created by the system as summarized in the table below:

File Type	File Name
Log File	<i>logllff-timestamp</i>
Accounting File	<i>actaaff-timestamp</i>

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the file-id
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
 - *yyyy* is the year (for example, 2006)
 - *mm* is the month number (for example, 12 for December)
 - *dd* is the day of the month (for example, 03 for the 3rd of the month)
 - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
 - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
 - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a *gz* extension.

When initialized, each file will contain:

- The *log-id* description.
- The time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

Default No default file IDs are defined.

Parameters *file-id* — The file identification number for the file, expressed as a decimal integer.

Values 1 — 99

location

Syntax **location** [*cflash-id* | *usb-flash-id*] [*backup-cflash-id*]
no location

Context config>log>file *file-id*

Description This command specifies the primary location where the log or billing file will be created.

When creating files, the primary location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space does become available, then the alarm condition will be cleared.

Use the **no** form of this command to revert to default settings.

Default Log files are created on cf1: and accounting files are created on cf1:.

Parameters *cflash-id* — Specify the primary location.

Values *cflash-id*: Values allowed for different platforms are as listed below:
7210 SAS-M and 7210 SAS-X: cf1:|uf1:

**7210 SAS-T, 7210 SAS-Mxp, and 7210 SAS-Sx - cf1:cf2:uf1:
7210 SAS-R6 and 7210 SAS-R12 - cf1:cf1-A:cf1-B:cf2:cf2-A:cf2-B:uf1:uf1-A: uf1-B:**

usb-flash-id — Specifies the USB location.

Values usb-flash-id: **Values allowed for different platforms are as listed below:**
7210 SAS-M and 7210 SAS-X: cf1:uf1:
7210 SAS-T, 7210 SAS-Mxp, and 7210 SAS-Sx - cf1:cf2:uf1:
7210 SAS-R6 and 7210 SAS-R12 - cf1:cf1-A:cf1-B:cf2:cf2-A:cf2-B:uf1:uf1-A: uf1-B:

backup-cflash-id — Specify the backup location.

Values backup-cflash-id: **Values allowed for different platforms are as listed below:**
7210 SAS-M and 7210 SAS-X: cf1:uf1:
7210 SAS-T, 7210 SAS-Mxp, and 7210 SAS-Sx - cf1:cf2:uf1:
7210 SAS-R6 and 7210 SAS-R12 - cf1:cf1-A:cf1-B:cf2:cf2-A:cf2-B:uf1:uf1-A: uf1-B:

rollover

Syntax	rollover <i>minutes</i> [retention <i>hours</i>] no rollover
Context	config>log>file <i>file-id</i>
Description	<p>This command configures how often an event or accounting log is rolled over or partitioned into a new file.</p> <p>An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the rollover time, expressed in minutes.</p> <p>The retention option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.</p> <p>When multiple rollover commands for a <i>file-id</i> are entered, the last command overwrites the previous command.</p>
Default	rollover 1440 retention 12
Parameters	<p><i>minutes</i> — The rollover time, in minutes.</p> <p>Values 5 — 10080</p>

retention hours. The retention period in hours, expressed as a decimal integer. The retention time is based on the time creation time of the file. The file becomes a candidate for removal once the creation datestamp + rollover time + retention time is less than the current timestamp.

Default 12

Values 1 — 500

Log Filter Commands

filter

Syntax	[no] filter <i>filter-id</i>
Context	config>log
Description	<p>This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.</p> <p>Filters are configured in the filter <i>filter-id</i> context and then applied to a log in the log-id <i>log-id</i> context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.</p> <p>Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.</p> <p>The no form of the command removes the filter association from log IDs which causes those logs to forward all events.</p>
Default	No event filters are defined.
Parameters	<p>filter-id — The filter ID uniquely identifies the filter.</p> <p>Values 1 — 1001</p>

default-action

Syntax	default-action {drop forward} no default-action
Context	config>log>filter <i>filter-id</i>
Description	<p>The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.</p> <p>When multiple default-action commands are entered, the last command overwrites the previous command.</p> <p>The no form of the command reverts the default action to the default value (forward).</p>
Default	default-action forward — The events which are not explicitly dropped by an event filter match are forwarded.
Parameters	<p>drop — The events which are not explicitly forwarded by an event filter match are dropped.</p> <p>forward — The events which are not explicitly dropped by an event filter match are forwarded.</p>

Log Filter Entry Commands

action

Syntax	action { drop forward } no action
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
Description	<p>This command specifies a drop or forward action associated with the filter entry. If neither drop nor forward is specified, the default-action will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.</p> <p>Multiple action statements entered will overwrite previous actions.</p> <p>The no form of the command removes the specified action statement.</p>
Default	Action specified by the default-action command will apply.
Parameters	<p>drop — Specifies packets matching the entry criteria will be dropped.</p> <p>forward — Specifies packets matching the entry criteria will be forwarded.</p>

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>log>filter <i>filter-id</i>
Description	<p>This command is used to create or edit an event filter entry. Multiple entries may be created using unique <i>entry-id</i> numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.</p> <p>Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.</p> <p>The no form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.</p>
Default	No event filter entries are defined. An entry must be explicitly configured.

Parameters *entry-id*. The entry ID uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 — 999

Log Filter Entry Match Commands

match

Syntax	[no] match
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
Description	<p>This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.</p> <p>If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.</p> <p>Use the application command to display a list of the valid applications.</p> <p>Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple match statements cannot be entered per entry.</p> <p>The no form of the command removes the match criteria for the <i>entry-id</i>.</p>
Default	No match context is defined.

application

Syntax	application {eq neq} application-id no application
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i> >match
Description	<p>This command adds an OS application as an event filter match criterion.</p> <p>An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES etc. Only one application can be specified. The latest application command overwrites the previous command.</p> <p>The no form of the command removes the application as a match criterion.</p>
Default	no application — No application match criterion is specified.
Parameters	eq neq — The operator specifying the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to

application-id — The application name string.

Values chassis|debug|efm_oam|eth_cfm|ering|filter|igmp_snooping|ip|isis|lag|ldp|lldp|logger|mirror|mpls|ntp|oam|ospf|port|route_policy|rsvp|security|snmp|stp|svcmgr|system|user|vrtr

number

Syntax **number** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *event-id*
no number

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an SR OS application event number as a match criterion. SR OS event numbers uniquely identify a specific logging event within an application. Only one **number** command can be entered per event filter entry. The latest **number** command overwrites the previous command. The **no** form of the command removes the event number as a match criterion.

Default **no event-number** — No event ID match criterion is specified.

Parameters **eq** | **neq** | **lt** | **lte** | **gt** | **gte** — This operator specifies the type of match. Valid operators are listed in the table below. Valid operators are:

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id — The event ID, expressed as a decimal integer.

Values 1 — 4294967295

router

Syntax	router { eq neq } <i>router-instance</i> [regex] no router
Context	config>log>filter>entry>match
Description	This command specifies the log event matches for the router.
Parameters	eq — Determines if the matching criteria should be equal to the specified value. neq — Determines if the matching criteria should not be equal to the specified value. <i>router-instance</i> — Specifies a router name up to 32 characters to be used in the match criteria. regex — Specifies the type of string comparison to use to determine if the log event matches the value of router command parameters. When the regex keyword is specified, the string in the router command is a regular expression string that will be matched against the subject string in the log event being filtered.

severity

Syntax	severity { eq neq lt lte gt gte } <i>severity-level</i> no severity
Context	config>log>filter>entry>match
Description	This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command. The no form of the command removes the severity match criterion.
Default	no severity — No severity level match criterion is specified.
Parameters	eq neq lt lte gt gte — This operator specifies the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

severity-level — The ITU severity level name. The following table lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Values cleared, intermediate, critical, major, minor, warning

subject

Syntax **subject** {**eq**|**neq**} *subject* [**regexp**]
no subject

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

The **no** form of the command removes the subject match criterion.

Default **no subject** — No subject match criterion specified.

Parameters **eq** | **neq** — This operator specifies the type of match. Valid operators are listed in the following table:

Operator	Notes
eq	equal to
neg	not equal to

subject — A string used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered.

When **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

Syslog Commands

syslog

Syntax	[no] syslog <i>syslog-id</i>
Context	config>log
Description	<p>This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.</p> <p>A valid <i>syslog-id</i> must have the target syslog host address configured.</p> <p>A maximum of 10 <i>syslog-id</i>'s can be configured.</p> <p>No log events are sent to a syslog target address until the <i>syslog-id</i> has been configured as the log destination (to) in the log-id node.</p>
Default	No syslog IDs are defined.
Parameters	<i>syslog-id</i> — The syslog ID number for the syslog destination, expressed as a decimal integer.
	Values 1 — 10

address

Syntax	address <i>ip-address</i> no address										
Context	config>log>syslog <i>syslog-id</i>										
Description	<p>This command adds the syslog target host IP address to/from a <i>syslog ID</i>.</p> <p>This parameter is mandatory. If no address is configured, syslog data cannot be forwarded to the syslog target host.</p> <p>Only one address can be associated with a <i>syslog-id</i>. If multiple addresses are entered, the last address entered overwrites the previous address.</p> <p>The same syslog target host can be used by multiple log IDs.</p> <p>The no form of the command removes the syslog target host IP address.</p>										
Default	no address — There is no syslog target host IP address defined for the <i>syslog ID</i> .										
Parameters	<i>ip-address</i> — The IP address of the syslog target host in dotted decimal notation.										
	Values										
	<table> <tr> <td>ipv4-address</td> <td>a.b.c.d</td> </tr> <tr> <td>ipv6-address</td> <td>x:x:x:x:x:x(x(eight 16-bit pieces))</td> </tr> <tr> <td></td> <td>x:x:x:x:x:d.d.d.d</td> </tr> <tr> <td></td> <td>x: [0..FFFF]H</td> </tr> <tr> <td></td> <td>d: [0..255]D</td> </tr> </table>	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
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										

facility

- Syntax** **facility** *syslog-facility*
no facility
- Context** config>log>syslog *syslog-id*
- Description** This command configures the facility code for messages sent to the syslog target host. Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last *facility-code* entered overwrites the previous facility-code. If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code. The **no** form of the command reverts to the default value.
- Default** **local7** — syslog entries are sent with the local7 facility code.
- Parameters** *syslog-facility* — The syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.
- Values** kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC3164, *The BSD syslog Protocol*, are listed in the table below.

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news
8	uucp
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0

Numerical Code	Facility Code
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7
Values	0 — 23

log-prefix

Syntax	log-prefix <i>log-prefix-string</i> no log-prefix
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command adds the string prepended to every syslog message sent to the syslog host.</p> <p>RFC3164, <i>The BSD syslog Protocol</i>, allows a alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.</p> <p>Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.</p> <p>The no form of the command removes the log prefix string.</p>
Default	no log-prefix — no prepend log prefix string defined.
Parameters	<i>log-prefix-string</i> — An alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

level

Syntax	level <i>syslog-level</i> no level
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.</p> <p>Only a single threshold level can be specified. If multiple levels are entered, the last level entered will overwrite the previously entered commands.</p>

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

Parameters *value* — The threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

Severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	0	emergency	system is unusable
3	1	alert	action must be taken immediately
4	2	critical	critical condition
5	3	error	error condition
6	4	warning	warning condition
	5	notice	normal but significant condition
1 cleared 2 indeterminate	6	info	informational messages
	7	debug	debug-level messages

port

Syntax **port** *port*
no port

Context config>log>syslog *syslog-id*

Description This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

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

Default **no port**

Parameters *port* — The value is the configured UDP port number used when sending syslog messages.

Values 0 — 65535

throttle-rate

Syntax	throttle-rate <i>events</i> [interval <i>seconds</i>] no throttle-rate
Context	config>log
Description	This command configures an event throttling rate.
Parameters	<i>events</i> — Specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, for example, the event drop count will be incremented. At the end of the throttle interval if any events have been dropped a trap notification will be sent. Values 10 — 20000 Default 500 <i>interval seconds</i> — Specifies the number of seconds that an event throttling interval lasts. Values 1 — 60 Default 1

SNMP Trap Groups

snmp-trap-group

Syntax	[no] snmp-trap-group <i>log-id</i>
Context	config>log
Description	<p>This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.</p> <p>A group specifies the types of SNMP traps and specifies the log ID which will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.</p> <p>To suppress the generation of all alarms and traps see the event-control command. To suppress alarms and traps that are sent to this log-id, see the filter command. Once alarms and traps are generated they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.</p> <p>The no form of the command deletes the SNMP trap group.</p>
Default	There are no default SNMP trap groups.
Parameters	<p><i>log-id</i> — The log ID value of a log configured in the log-id context. Alarms and traps cannot be sent to the trap receivers until a valid <i>log-id</i> exists.</p> <p>Values 1 — 100</p>

snmp-dying-gasp

Syntax	snmp-dying-gasp primary <i>trap-target-group-num trap-target-name</i> [secondary { <i>trap-target-group-num trap-target-name</i> }] [tertiary { <i>trap-target-group-num trap-target-name</i> }] no snmp-dying-gasp
Context	config>log
Description	<p>This command enables user to notify the SNMP trap server about node power failure. On power failure, the system sends dying gasp traps to the configured SNMP trap servers. Up to three SNMP trap servers can be configured to receive the trap. The traps are sent in the following order:</p> <ol style="list-style-type: none"> 1. Primary SNMP trap receiver. 2. Secondary SNMP trap receiver. 3. Tertiary SNMP trap receiver. <p>When this command is enabled, the node does not generate EFM OAM dying gasp message even if EFM OAM is enabled. In other words, generation of SNMP dying gasp trap is mutually exclusive to use of EFM OAM dying gasp message. By default, the system generates EFM OAM dying gasp</p>

message to remain compatible with older version of the software releases. User needs to explicitly configure the system to send out an SNMP trap on loss of power to the node, using this command.

The no form of the command disables generation of SNMP trap message. It enables generation of EFM OAM dying gasp on access-uplink ports, if EFM OAM is enabled on those ports. Generation of SNMP dying gasp trap is disabled by default.

Typically, SNMP traps are generated only if user configures a log to direct the system log events to SNMP. For SNMP dying gasp trap, it is not required to do so. The DSCP value used by a SNMP Dying Gasp packet is AF (Assured Forwarding class, value 22).

NOTES:

- System IP address must be configured. The node uses it for generating the Dying Gasp traps. If It is not configured SNMP dying gasp traps are not generated.
- When sending out SNMP dying gasp traps, one of the available routes in either the management routing instance or the base routing instance is used to resolve the next-hop gateway IP address to reach the trap-server destinations configured under primary, secondary and tertiary trap-targets. The route to the destination is always searched first in the management routing instance and if not found, the routes in the base routing instance is looked up. Configuration of route-preference does not change this behavior (that is, the order of route lookup does not change).

Default Disabled

Parameters **primary** *trap-target-group-num* *trap-target-name* — Specify the primary SNMP trap receiver to which the system will address the SNMP trap to. The *trap-target-group-num* must correspond to one of the SNMP trap group configuration under **config> log> snmp-trap-group** *trap-num*. The 'target-name' must correspond to one of the SNMP trap receiver target configured under **config> log> snmp-trap-group** *trap-num* **trap-target** *target-name*.

trap-target-group-num — The trap target group number, expressed as a decimal integer.

Values 1 — 100

trap-target-name — The trap target name, specified as a string of characters.

Up to 28 characters
secondary *trap-target-group-num* *trap-target-name* — Specify the secondary SNMP trap receiver to which the system will address the SNMP trap to. The *trap-target-group-num* must correspond to one of the SNMP trap group configuration under **config> log> snmp-trap-group** *trap-num*. The 'target-name' must correspond to one of the SNMP trap receiver target configured under **config> log> snmp-trap-group** *trap-num* **trap-target** *target-name*.

trap-target-group-num — The trap target group number, expressed as a decimal integer.

Values 1 — 100

trap-target-name — The trap target name, specified as a string of characters.

Values Up to 28 characters

tertiary *trap-target-group-num* *trap-target-name* — Specify the tertiary SNMP trap receiver to which the system will address the SNMP trap too. The *trap-target-group-num* must correspond to one of the SNMP trap group configuration under **config> log> snmp-trap-group** *trap-num*. The 'target-name' must correspond to one of the SNMP trap receiver target configured under **config> log> snmp-trap-group** *<trap-num>* **trap-target** *<target-name>*.

trap-target-group-num — The trap target group number, expressed as a decimal integer.

Values 1 — 100

trap-target-name — The trap target name, specified as a string of characters.

Values Up to 28 characters

trap-target

Syntax	trap-target <i>name</i> [address <i>ip-address</i>] [port <i>port</i>] [snmpv1 snmpv2c snmpv3] notify-community <i>communityName</i> <i>snmpv3SecurityName</i> [security-level { no-auth-no-privacy auth-no-privacy privacy }] [replay] no trap-target <i>name</i>
Context	config>log>snmp-trap-group
Description	<p>This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.</p> <p>Before an SNMP trap can be issued to a trap receiver, the log-id, snmp-trap-group and at least one trap-target must be configured.</p> <p>The trap-target command is used to add/remove a trap receiver from an snmp-trap-group. The operational parameters specified in the command include:</p> <ul style="list-style-type: none"> • The IP address of the trap receiver • The UDP port used to send the SNMP trap • SNMP version • SNMP community name for SNMPv1 and SNMPv2c receivers. • Security name and level for SNMPv3 trap receivers. <p>A single snmp-trap-group <i>log-id</i> can have multiple trap-receivers. Each trap receiver can have different operational parameters.</p> <p>An address can be configured as a trap receiver more than once as long as a different port is used for each instance.</p> <p>To prevent resource limitations, only configure a maximum of 10 trap receivers.</p> <p>Note that if the same trap-target <i>name</i> port <i>port</i> parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different <i>notify-community</i> value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each 7210 SAS event log when multiple event logs are directed to the same IP address and port destination.</p> <p>The no form of the command removes the SNMP trap receiver from the SNMP trap group.</p>
Default	No SNMP trap targets are defined.
Parameters	<i>name</i> — Specifies the name of the trap target up to 28 characters in length.

address *ip-address* — The IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group.

Values

ipv4-address	a.b.c.d (host bits must be 0)
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

port *port* — The destination UDP port used for sending traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address then multiple ports must be configured.

Default 162

Values 1 — 65535

snmpv1 | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1**, then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c**, then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Pre-existing conditions are checked before the `snmpv3SecurityName` is accepted. These are:

- The user name must be configured.
- The v3 access group must be configured.
- The v3 notification view must be configured.

Default snmpv3

Values snmpv1, snmpv2c, snmpv3

notify-community *community* | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If no **notify-community** is configured, then no alarms nor traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community — The community string as required by the **snmpv1** or **snmpv2c** trap receiver. The community string can be an ASCII string up to 31 characters in length.

security-name — The *security-name* as defined in the `config>system>security>user` context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

security-level {*no-auth-no-privacy* | *auth-no-privacy* | *privacy*} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

Default no-auth-no-privacy. This parameter can only be configured if SNMPv3 is also configured.

Values no-auth-no-privacy, auth-no-privacy, privacy

replay — Enables replay of missed events to target. If replay is applied to an SNMP trap target address, the address is monitored for reachability. Reachability is determined by whether or not there is a route in the routing table by which the target address can be reached. Before sending a trap to a target address, the SNMP module asks the PIP module if there is either an in-band or out-of-band route to the target address. If there is no route to the SNMP target address, the SNMP module saves the sequence-id of the first event that will be missed by the trap target. When the routing table changes again so that there is now a route by which the SNMP target address can be reached, the SNMP module replays (for example, retransmits) all events generated to the SNMP notification log while the target address was removed from the route table.

Note: The route table changes the convergence time so it is possible that one or more events may be lost at the beginning or end of a replay sequence.

Logging Destination Commands

filter

Syntax	filter <i>filter-id</i> no filter
Context	config>log>log-id <i>log-id</i>
Description	<p>This command adds an event filter policy with the log destination.</p> <p>The filter command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.</p> <p>An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination snmp-trap-group.</p> <p>The application of filters for debug messages is limited to application and subject only.</p> <p>Accounting records cannot be filtered using the filter command.</p> <p>Only one filter-id can be configured per log destination.</p> <p>The no form of the command removes the specified event filter from the <i>log-id</i>.</p>
Default	no filter — No event filter policy is specified for a <i>log-id</i> .
Parameters	<p><i>filter-id</i>. The event filter policy ID is used to associate the filter with the <i>log-id</i> configuration. The event filter policy ID must already be defined in config>log>filter <i>filter-id</i>.</p> <p>Values 1 — 1001</p>

from

Syntax	from {[main] [security] [change] [debug-trace] } no from
Context	config>log>log-id <i>log-id</i>
Description	<p>This command selects the source stream to be sent to a log destination.</p> <p>One or more source streams must be specified. The source of the data stream must be identified using the from command before you can configure the destination using the to command. The from command can identify multiple source streams in a single statement (for example: from main change debug-trace).</p> <p>Only one from command may be entered for a single <i>log-id</i>. If multiple from commands are configured, then the last command entered overwrites the previous from command.</p> <p>The no form of the command removes all previously configured source streams.</p>

Default	No source stream is configured.
Parameters	<p><i>main</i> — Instructs all events in the main event stream to be sent to the destination defined in the to command for this destination <i>log-id</i>. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the filter command.</p> <p><i>security</i> — Instructs all events in the security event stream to be sent to the destination defined in the to command for this destination <i>log-id</i>. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the filter command.</p> <p><i>change</i> — Instructs all events in the user activity stream to be sent to the destination configured in the to command for this destination <i>log-id</i>. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the filter command.</p> <p><i>debug-trace</i> — Instructs all debug-trace messages in the debug stream to be sent to the destination configured in the to command for this destination <i>log-id</i>. Filters applied to debug messages are limited to application and subject.</p>

log-id

Syntax	[no] log-id <i>log-id</i>
Context	config>log
Description	<p>This command creates a context to configure destinations for event streams.</p> <p>The log-id context is used to direct events, alarms/traps, and debug information to respective destinations.</p> <p>A maximum of 10 logs can be configured.</p> <p>Before an event can be associated with this log-id, the from command identifying the source of the event must be configured.</p> <p>Only one destination can be specified for a <i>log-id</i>. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.</p> <p>Use the event-control command to suppress the generation of events, alarms, and traps for all log destinations.</p> <p>An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.</p> <p>Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages. Log-ID 100 captures log messages with a severity level of major and above.</p> <p>Note that Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.</p>

Configuration Commands

The **no** form of the command deletes the log destination ID from the configuration.

Default No log destinations are defined.

Parameters *log-id* — The log ID number, expressed as a decimal integer.

Values 1 — 100

to console

Syntax **to console**

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all the entries are dropped.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

to file

Syntax **to file** *log-file-id*

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a specified file.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

Parameters *log-file-id* — Instructs the events selected for the log ID to be directed to the *log-file-id*. The characteristics of the *log-file-id* referenced here must have already been defined in the **config>log>file** *log-file-id* context.

Values 1 — 99

to memory

Syntax	to memory [<i>size</i>]				
Context	config>log>log-id <i>log-id</i>				
Description	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a memory log. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>				
Default	none				
Parameters	<p><i>size</i> — The <i>size</i> parameter indicates the number of events that can be stored in the memory.</p> <table> <tr> <td>Default</td> <td>100</td> </tr> <tr> <td>Values</td> <td>50 — 1024</td> </tr> </table>	Default	100	Values	50 — 1024
Default	100				
Values	50 — 1024				

to session

Syntax	to session
Context	config>log>log-id <i>log-id</i>
Description	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the current console or telnet session. This command is only valid for the duration of the session. When the session is terminated the log ID is removed. A log ID with a <i>session</i> destination is not saved in the configuration file.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
Default	none

to snmp

Syntax	to snmp [<i>size</i>]
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the alarms and traps to be directed to the snmp-trap-group associated with <i>log-id</i>.</p> <p>A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the <i>log-id</i>.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
Default	none
Parameters	<i>size</i> — The <i>size</i> parameter defines the number of events stored in this memory log.
	Default 100
	Values 50 — 1024

to syslog

Syntax	to syslog <i>syslog-id</i>
Context	config>log>log-id
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1k bytes.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
Default	none
Parameters	<i>syslog-id</i> — Instructs the events selected for the log ID to be directed to the <i>syslog-id</i> . The characteristics of the <i>syslog-id</i> referenced here must have been defined in the config>log>syslog <i>syslog-id</i> context.
	Values 1 — 10

time-format

Syntax	time-format {local utc}
Context	config>log>log-id
Description	This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.
Default	utc
Parameters	local — Specifies that timestamps are written in the system's local time. utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Accounting Policy Commands

accounting-policy

Syntax	accounting-policy <i>policy-id</i> no accounting-policy <i>policy-id</i>
Context	config>log
Description	<p>This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.</p> <p>Access accounting policies are policies that can be applied to one or more SAPs or access ports. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs or access ports where this policy is applied.</p> <p>If an accounting policy is not specified on a SAP or an access port, then accounting records are produced in accordance with the access policy designated as the default. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.</p> <p>Network accounting policies are policies that can be applied to one or more network ports, network IP interfaces and SDPs. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports, IP interfaces or SDPs where this policy is applied.</p> <p>If no accounting policy is defined on a network port, network IP interface and SDP, accounting records will be produced in accordance with the default network policy as designated with the default command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.</p> <p>In the 7210 SAS M, a total of 21 accounting records are available. There are five types of accounting policies:</p> <ul style="list-style-type: none">• Access• Access port• Network• Network interface• SDP <p>When creating accounting policies, one access, one access port, one network, one network interface and one SDP accounting-policy can be defined as default. If statistics collection is enabled on an accounting object, and no accounting policy is applied, then the respective default accounting policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.</p> <p>The no form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.</p>
Default	No default accounting policy is defined.

Parameters *policy-id* — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 — 99

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context config>log>acct-policy

Description This command configures the accounting collection interval.

Parameters *minutes* — Specifies the interval between collections, in minutes.

Values 5 — 120
 A range of 1 — 4 is only allowed when the record type is set to SAA.

default

Syntax [**no**] **default**

Context config>log>accounting-policy

Description This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.

If no accounting policy is defined on an access or network object, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

When creating accounting policies, one access, one access port, one network, one network interface and one SDP accounting policy can be defined as default.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of the command removes the default policy designation from the policy ID. The accounting policy will be removed from all access or network object ports that do not have this policy explicitly defined.

record

- Syntax** `[no] record record-name`
- Context** `config>log>accounting-policy policy-id`
- Description** This command adds the accounting record type to the accounting policy to be forwarded to the configured accounting file. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

To configure an accounting policy for SAPs, select the access type accounting records such as `service-ingress-packets`; for access ports select access port type records such as `access-egress-packets`; for network ports select network type records such as `network-egress-packets`; for IP interfaces select network interface type records such as `network-interface-ingress-packets`; and for SDP and SDP bindings select SDP type records such as `complete-sdp-ingress-egress`.

If the change required modifies the record from one type to another, then the old record name must be removed using the **no** form of this command.

Only one record may be configured in a single accounting policy. For example, if an accounting-policy is configured with an **access-egress-octets** record, in order to change it to **service-ingress-octets**, use the **no record** command under the accounting-policy to remove the old record and then enter the **service-ingress-octets** record.

Note that collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of the command removes the record type from the policy.

- Default** No accounting record is defined
- Parameters** `record-name` — The accounting record name. The following table lists the accounting record names available and the default collection interval.

Sample output for 7210 SAS-M:

```
*A:7210-SAS-M>show>log# accounting-records
=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1         service-ingress-octets                       5
2         service-egress-octets                       5
3         service-ingress-packets                     5
4         service-egress-packets                     5
5         network-ingress-octets                      15
6         network-egress-octets                      15
7         network-ingress-packets                     15
8         network-egress-packets                     15
10        combined-service-ingress                    5
```

```

11      combined-network-ing-egr-octets      15
13      complete-service-ingress-egress     5
14      combined-sdp-ingress-egress         5
15      complete-sdp-ingress-egress         5
32      saa                                  5
33      network-interface-ingress-octets    15
34      network-interface-ingress-packets   15
35      combined-network-interface-ingress  15
36      access-egress-packets               5
37      access-egress-octets                5
38      combined-access-egress              5
39      combined-network-egress             15
40      combined-service-egress             5
=====
*A:7210-SAS-M>show>log#

```

Sample output for 7210 SAS-X:

```

*A:7210-SAS-X>show>log# accounting-records

=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1      service-ingress-octets                         5
2      service-egress-octets                         5
3      service-ingress-packets                        5
4      service-egress-packets                         5
5      network-ingress-octets                         15
6      network-egress-octets                         15
7      network-ingress-packets                        15
8      network-egress-packets                        15
10     combined-service-ingress                        5
11     combined-network-ing-egr-octets                15
13     complete-service-ingress-egress                5
14     combined-sdp-ingress-egress                    5
15     complete-sdp-ingress-egress                    5
32     saa                                              5
33     network-interface-ingress-octets              15
34     network-interface-ingress-packets            15
35     combined-network-interface-ingress            15
39     combined-network-egress                       15
40     combined-service-egress                       5
=====
*A:7210-SAS-X>show>log#

```

Sample output for 7210 SAS-Mxp:

```

*A:sim_dutc>show>log# accounting-records

=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----

```

Configuration Commands

```
1      service-ingress-octets      5
2      service-egress-octets       5
3      service-ingress-packets     5
4      service-egress-packets      5
5      network-ingress-octets      15
6      network-egress-octets       15
7      network-ingress-packets     15
8      network-egress-packets      15
10     combined-service-ingress    5
11     combined-network-ing-egr-octets 15
13     complete-service-ingress-egress 5
14     combined-sdp-ingress-egress  5
15     complete-sdp-ingress-egress  5
32     saa                          5
101    network-interface-ingress-octets 15
102    network-interface-ingress-packets 15
103    combined-network-interface-ingress 15
104    access-egress-packets       5
105    access-egress-octets        5
106    combined-access-egress      5
107    combined-network-egress     15
108    combined-service-egress     5
=====
*A:sim_dutc>show>log#
```

Sample output for 7210 SAS-Sx:

```
*7210SAS>show>log# accounting-records

=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1      service-ingress-octets                       5
2      service-egress-octets                        5
3      service-ingress-packets                      5
4      service-egress-packets                       5
5      network-ingress-octets                       15
6      network-egress-octets                        15
7      network-ingress-packets                      15
8      network-egress-packets                       15
10     combined-service-ingress                      5
11     combined-network-ing-egr-octets                15
13     complete-service-ingress-egress                5
14     combined-sdp-ingress-egress                    5
15     complete-sdp-ingress-egress                    5
32     saa                                             5
101    network-interface-ingress-octets              15
102    network-interface-ingress-packets              15
103    combined-network-interface-ingress              15
104    access-egress-packets                          5
105    access-egress-octets                           5
106    combined-access-egress                          5
107    combined-network-egress                         15
```

```

108      combined-service-egress      5
=====
*A:7210SAS>show>log#

```

to

Syntax	to file <i>file-id</i>
Context	config>log>accounting-policy <i>policy-id</i>
Description	This command specifies the destination for the accounting records selected for the accounting policy.
Default	No destination is specified.
Parameters	<p><i>file-id</i> — The <i>file-id</i> option specifies the destination for the accounting records selected for this destination. The characteristics of the file-id must have already been defined in the config>log>file context. A file-id can only be used once.</p> <p>The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.</p> <p>If the to command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.</p> <p>Values 1 — 99</p>

log-memory

Syntax	log-memory [no] log-memory
Context	config>log>accounting-policy
Description	<p>If the user specifies use of log-memory, the system allocates some RAM (that is, volatile memory) as a temporary storage to write accounting records every collection-interval. The accounting records are moved from the temporary storage to the accounting file on non-volatile memory (that is, flash), when either the rollover-interval expires or when temporary storage location gets full.</p> <p>NOTE: The accounting records held in the temporary storage is lost on a reboot (either due to loss of power or due to user action).</p>
Default	By default an accounting record is not configured to use temporary storage.
Parameters	<p><i>Size</i> — The user can request the system to allocate more RAM memory for temporary storage by using the size parameter. The system allocates the memory if its within the system limit available for use with accounting records. By default, the system allocates 128KB of memory.</p>

Show Commands

accounting-policy

Syntax	accounting-policy [<i>acct-policy-id</i>] [access network]
Context	show>log
Description	This command displays accounting policy information.
Parameters	<p><i>policy-id</i> — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.</p> <p>Values 1 — 99</p> <p>access — Only displays access accounting policies.</p> <p>network — Only displays network accounting policies.</p>
Output	Accounting Policy Output — The following table describes accounting policy output fields.

Table 34: Show Accounting Policy Output Fields

Label	Description
Policy ID	The identifying value assigned to a specific policy.
Type	<p>Identifies accounting record type forwarded to the configured accounting file.</p> <p><i>access</i> — Indicates that the policy is an access accounting policy.</p> <p><i>network</i> — Indicates that the policy is a network accounting policy.</p> <p><i>sdp</i> — Indicates that the policy is meant to collect accounting stats for SDPs and spoke SDPs.</p> <p><i>access port</i> — Indicates that the policy is an access port accounting policy which can be used to collect accounting records only for access ports.</p> <p><i>network interface</i> — Indicates that the policy is an network Interface accounting policy which can be used to collect accounting records only for network IP interface.</p> <p><i>none</i> — Indicates no accounting record types assigned.</p>
Def	<p><i>Yes</i> — Indicates that the policy is a default access or network policy.</p> <p><i>No</i> — Indicates that the policy is not a default access or network policy.</p>

Table 34: Show Accounting Policy Output Fields (Continued)

Label	Description (Continued)
Admin State	Displays the administrative state of the policy. Up – Indicates that the policy is administratively enabled. Down – Indicates that the policy is administratively disabled.
Oper State	Displays the operational state of the policy. Up – Indicates that the policy is operationally up. Down – Indicates that the policy is operationally down.
Intvl	Displays the interval, in minutes, in which statistics are collected and written to their destination. The default depends on the record name type.
File ID	The log destination.
Record Name	The accounting record name which represents the configured record type.
Log-Memory	If the values shown is 'Yes', it indicates that temporary volatile memory is in use for this accounting policy. If it displays 'No', the temporary volatile memory is not in use for this accounting policy.
Log-Memory Size	The amount of temporary volatile memory in use for this accounting policy.
This policy is applied to	Specifies the entity where the accounting policy is applied.

Sample Output:

```
*A:7210-SAS-M>show>log# accounting-policy
=====
Accounting Policies
=====

Policy Type      Def Admin Oper  Intvl File Record Name
Id              State State   State   Id
-----
1      access    No  Down  Down  5    1    combined-service-ingress

Description      : (Not Specified)
Log-Memory       : Yes
Log-Memory Size  : 128 KB

Data Loss Count  : 0                      Data Loss TimeStamp: N/A
-----

This policy is applied to:
  Svc :101                      SAP:lag-3:101.101                      Collect-Stats
```

```

Svc :102          SAP:lag-3:102.102          Collect-Stats
Svc :103          SAP:lag-3:103.103          Collect-Stats
....

```

accounting-records

- Syntax** `accounting-records`
- Context** `show>log`
- Description** This command displays accounting policy record names.
- Output** **Accounting Records Output.** The following table describes accounting records output fields.

Table 35: Accounting Policy Output Fields

Label	Description
Record #	The record ID that uniquely identifies the accounting policy, expressed as a decimal integer.
Record Name	The accounting record name.
Def. Interval	The default interval, in minutes, in which statistics are collected and written to their destination.

Sample output for 7210 SAS-M:

```

*A:7210-SAS-M>show>log# accounting-records

=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1      service-ingress-octets                          5
2      service-egress-octets                           5
3      service-ingress-packets                          5
4      service-egress-packets                           5
5      network-ingress-octets                            15
6      network-egress-octets                             15
7      network-ingress-packets                           15
8      network-egress-packets                             15
10     combined-service-ingress                           5
11     combined-network-ing-egr-octets                    15
13     complete-service-ingress-egress                    5
14     combined-sdp-ingress-egress                         5
15     complete-sdp-ingress-egress                         5
32     saa                                                  5
33     network-interface-ingress-octets                   15
34     network-interface-ingress-packets                  15
35     combined-network-interface-ingress                 15

```

Show Commands

```
36      access-egress-packets          5
37      access-egress-octets           5
38      combined-access-egress         5
39      combined-network-egress        15
40      combined-service-egress        5
=====
*A:7210-SAS-M>show>log#
```

Sample output for 7210 SAS-X:

```
*A:7210-SAS-X>show>log# accounting-records

=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1      service-ingress-octets                       5
2      service-egress-octets                        5
3      service-ingress-packets                      5
4      service-egress-packets                       5
5      network-ingress-octets                       15
6      network-egress-octets                        15
7      network-ingress-packets                      15
8      network-egress-packets                       15
10     combined-service-ingress                       5
11     combined-network-ing-egr-octets              15
13     complete-service-ingress-egress              5
14     combined-sdp-ingress-egress                  5
15     complete-sdp-ingress-egress                  5
32     saa                                           5
33     network-interface-ingress-octets             15
34     network-interface-ingress-packets            15
35     combined-network-interface-ingress           15
39     combined-network-egress                      15
40     combined-service-egress                      5
=====
*A:7210-SAS-X>show>log#
```

applications

Syntax	applications
Context	show>log
Description	This command displays a list of all application names that can be used in event-control and filter commands.
Output	Sample Output

```
A:ALA-1# show log applications
=====
Log Event Application Names
=====
Application Name
-----
CCAG
```

```

CHASSIS
CPMHWFILTER
DHCP
DEBUG
DOT1X
FILTER
IGMP
IGMP_SNOOPING
IP
ISIS
LAG
LDP
LOGGER
MIRROR
MPLS
OAM
OSPF
PORT
PPP
QOS
RIP
ROUTE_POLICY
RSVP
SECURITY
SNMP
STP
SVCMMGR
SYSTEM
USER
VRRP
VRTR
=====
A:ALA-1#

```

event-control

- Syntax** `event-control [application-id [event-name | event-number]]`
- Context** `show>log`
- Description** This command displays event control settings for events including whether the event is suppressed or generated and the severity level for the event.
If no options are specified all events, alarms and traps are listed.
- Parameters** **application-id** — Only displays event control for the specified application.
- Default** All applications.
- Values** chassis|debug|efm_oam|eth_cfm|ering|filter|igmp_snooping|ip|isis|lag|ldp|lldp|logger|mirror|mpls|ntp|oam|ospf|port|route_policy|rsvp|security|snmp|stp|svcmgr|system|user|vrtr
- event-name** — Only displays event control for the named application event.
- Default** All events for the application.

event-number — Only displays event control for the specified application event number.

Default All events for the application.

Values 0 up to 4294967295

Output **Show Event Control Output** — The following table describes the output fields for the event control.

Label	Description
Application	The application name.
ID#	The event ID number within the application. L ID# — An “L” in front of an ID represents event types that do not generate an associated SNMP notification. Most events do generate a notification, only the exceptions are marked with a preceding “L”.
Event Name	The event name.
P	CL — The event has a cleared severity/priority. CR — The event has critical severity/priority. IN — The event has indeterminate severity/priority. MA — The event has major severity/priority. MI — The event has minor severity/priority. WA — The event has warning severity/priority.
g/s	gen — The event will be generated/logged by event control. sup — The event will be suppressed/dropped by event control. thr — Specifies that throttling is enabled.
Logged	The number of events logged/generated.
Dropped	The number of events dropped/suppressed.

Sample Output

```
*A:SAS-M>show>log# event-control
=====
Log Events
=====
Application
ID#      Event Name                               P  g/s   Logged   Dropped
-----
BGP:
  2001  bgpEstablished                          MI  gen    0         0
  2002  bgpBackwardTransition                   WA  gen    0         0
  2003  tBgpMaxPrefix90                         WA  gen    0         0
  2004  tBgpMaxPrefix100                        CR  gen    0         0
L  2005  sendNotification                         WA  gen    0         0
L  2006  receiveNotification                      WA  gen    0         0
L  2007  bgpInterfaceDown                         WA  gen    0         0
```

L	2008	bgpConnNoKA	WA	gen	0	0
L	2009	bgpConnNoOpenRcvd	WA	gen	0	0
L	2010	bgpRejectConnBadLocAddr	WA	gen	0	0
L	2011	bgpRemoteEndClosedConn	WA	gen	0	0
L	2012	bgpPeerNotFound	WA	gen	0	0
L	2013	bgpConnMgrTerminated	WA	gen	0	0
L	2014	bgpTerminated	WA	gen	0	0
L	2015	bgpNoMemoryPeer	CR	gen	0	0
L	2016	bgpVariableRangeViolation	WA	gen	0	0
L	2017	bgpCfgViol	WA	gen	0	0
	2018	tBgpPeerGRStatusChange	WA	gen	0	0
	2019	tBgpNgEstablished	MI	gen	0	0
	2020	tBgpNgBackwardTransition	WA	gen	0	0
	2021	tBgpPeerNgHoldTimeInconsistent	WA	gen	0	0
CHASSIS:						
	2001	cardFailure	MA	gen	0	0
	2002	cardInserted	MI	gen	5	0
	2003	cardRemoved	MI	gen	0	0
	2004	cardWrong	MI	gen	0	0
	2005	EnvTemperatureTooHigh	MA	gen	0	0
	2006	fanFailure	CR	gen	0	0
	2007	powerSupplyOverTemp	CR	gen	0	0
	2008	powerSupplyAcFailure	CR	gen	0	0
	2009	powerSupplyDcFailure	CR	gen	0	0
	2010	powerSupplyInserted	MA	gen	1	0
	2011	powerSupplyRemoved	MA	gen	0	0
	2012	redPrimaryCPMFail	CR	gen	0	0
	2016	clearNotification	MA	gen	0	0
	2017	syncIfTimingHoldover	CR	gen	0	0
	2018	syncIfTimingHoldoverClear	CR	gen	0	0
	2019	syncIfTimingRef1Alarm	MI	gen	0	0
	2020	syncIfTimingRef1AlarmClear	MI	gen	0	0
	2021	syncIfTimingRef2Alarm	MI	gen	0	0
	2022	syncIfTimingRef2AlarmClear	MI	gen	0	0
	2023	flashDataLoss	MA	gen	0	0
	2024	flashDiskFull	MA	gen	0	0
	2025	softwareMismatch	MA	gen	0	0
	2026	softwareLoadFailed	MA	gen	0	0
	2027	bootloaderMismatch	MA	gen	1	0
	2028	bootromMismatch	MA	gen	0	0
	2029	fpgaMismatch	MA	gen	0	0
	2030	syncIfTimingBITSAlarm	MI	gen	0	0
	2031	syncIfTimingBITSAlarmClear	MI	gen	0	0
	2032	cardUpgraded	MA	gen	0	0
	2033	cardUpgradeInProgress	MA	gen	0	0
	2034	cardUpgradeComplete	MA	gen	0	0
	2050	powerSupplyInputFailure	CR	gen	0	0
	2051	powerSupplyOutputFailure	CR	gen	0	0
	2052	mdaHiBwMulticastAlarm	MI	gen	0	0
	2056	mdaCfgNotCompatible	MA	gen	0	0
	2057	cardSyncFileNotPresent	MI	gen	0	0
	2058	tmnxEqMdaXplError	MI	sup	0	0
	2059	tmnxEqCardPChipError	MI	sup	0	0
	2060	tmnxEqCardSoftResetAlarm	MI	gen	0	0
	2061	tmnxEqMdaSyncENotCompatible	MA	gen	0	0
	2062	tmnxIPsecIsaGrpActiveIsaChgd	MI	gen	0	0
	2063	tmnxEqCardPChipMemoryEvent	MI	sup	0	0
	2064	tmnxIPsecIsaGrpUnableToSwitch	MI	gen	0	0
	2065	tmnxIPsecIsaGrpTnlLowWMark	MI	gen	0	0

Show Commands

```

2066 tmnxIPsecIsaGrpTnlHighWMark      MI gen      0      0
2067 tmnxIPsecIsaGrpTnlMax            MI gen      0      0
2076 tmnxEqCardPChipCamEvent          CR gen      0      0
2078 tmnxEqHwEnhancedCapability        MA gen      0      0
2068 tmnxEqSyncIfTimingRef1Quality     MI gen      0      0
2069 tmnxEqSyncIfTimingRef2Quality     MI gen      0      0
2072 tmnxEqSyncIfTimingRefSwitch       MI gen      0      0
2077 tmnxEqSyncIfTimingSystemQuality   MI gen      1      0
3001 tmnxSasAlarminput1StateChanged    MA gen      0      0
3002 tmnxSasAlarminput2StateChanged    MA gen      0      0
3003 tmnxSasAlarminput3StateChanged    MA gen      0      0
3004 tmnxSasAlarminput4StateChanged    MA gen      0      0
3000 EnvTemperatureTooLow             MA gen      0      0
DEBUG:
L 2001 traceEvent                     MI gen      0      0
EFM_OAM:
2001 tmnxDot3OamPeerChanged           MI gen      0      0
2002 tmnxDot3OamLoopDetected          MI gen      0      0
2003 tmnxDot3OamLoopCleared           MI gen      0      0
2008 dot3OamNonThresholdEvent         MI gen      0      0
2902 tmnxDyingGasp                    MI gen      0      0
ETH_CFM:
2001 dotlagCfmFaultAlarm              MI gen      0      0
2002 tmnxDotlagCfmMepLbmTestComplete  MI gen      0      0
2003 tmnxDotlagCfmMepLtmTestComplete  MI gen      0      0
2004 tmnxDotlagCfmMepEthTestComplete  MI gen      0      0
2005 tmnxDotlagCfmMepDMTestComplete   MI gen      0      0
2006 tmnxDotlagCfmMepAisStateChanged  MI gen      0      0
2007 tmnxDotlagCfmMipEvaluation       MI gen      0      0
ERING:
2001 tmnxEthRingPathFwdStateChange    MI gen      0      0
2002 tmnxEthRingApsPrvsNRaiseAlarm    MI gen      0      0
2003 tmnxEthRingApsPrvsNClearAlarm    MI gen      0      0
ETUN:
2001 tmnxEthTunnelApsCfgRaiseAlarm    MI gen      0      0
2002 tmnxEthTunnelApsCfgClearAlarm    MI gen      0      0
2003 tmnxEthTunnelApsPrvsNRaiseAlarm  MI gen      0      0
2004 tmnxEthTunnelApsPrvsNClearAlarm  MI gen      0      0
2005 tmnxEthTunnelApsNoRspRaiseAlarm  MI gen      0      0
2006 tmnxEthTunnelApsNoRspClearAlarm  MI gen      0      0
2007 tmnxEthTunnelApsSwitchoverAlarm  MI gen      0      0
FILTER:
2001 tIPFilterPBRPacketsDrop          WA gen      0      0
2002 tFilterEntryActivationFailed      WA gen      0      0
2003 tFilterEntryActivationRestored    WA gen      0      0
IGMP_SNOOPING:
2001 sapIgmpSnpgGrpLimitExceeded      WA gen      0      0
2002 sapIgmpSnpgMcacPlcyDropped       WA gen      0      0
2003 sdpBndIgmpSnpgGrpLimitExceeded   WA gen      0      0
2004 sdpBndIgmpSnpgMcacPlcyDropped    WA gen      0      0
2005 sapIgmpSnpgMcsFailure            WA gen      0      0
2006 sapIgmpSnpgSrcLimitExceeded      WA gen      0      0
2007 sdpBndIgmpSnpgSrcLimitExceeded    WA gen      0      0
IP:
L 2001 clearRTMError                  MI gen      0      0
L 2002 ipEtherBroadcast               MI gen      0      0
L 2003 ipDuplicateAddress              MI gen      0      0
L 2004 ipArpInfoOverwritten            MI gen      0      0
L 2005 fibAddFailed                    MA gen      0      0
L 2006 qosNetworkPolicyMallocFailed    MA gen      0      0
L 2007 ipArpBadInterface               MI gen      0      0

```

L	2008	ipArpDuplicateIpAddress	MI	gen	0	0
L	2009	ipArpDuplicateMacAddress	MI	gen	0	0
L	2010	ipAnyDuplicateAddress	MI	gen	0	0
ISIS:						
	2001	vRtrIisisDatabaseOverload	WA	gen	0	0
	2002	vRtrIisisManualAddressDrops	WA	gen	0	0
	2003	vRtrIisisCorruptedLSPDetected	WA	gen	0	0
	2004	vRtrIisisMaxSeqExceedAttempt	WA	gen	0	0
	2005	vRtrIisisIDLenMismatch	WA	gen	0	0
	2006	vRtrIisisMaxAreaAdrsMismatch	WA	gen	0	0
	2007	vRtrIisisOwnLSPPurge	WA	gen	0	0
	2008	vRtrIisisSequenceNumberSkip	WA	gen	0	0
	2009	vRtrIisisAutTypeFail	WA	gen	0	0
	2010	vRtrIisisAuthFail	WA	gen	0	0
	2011	vRtrIisisVersionSkew	WA	gen	0	0
	2012	vRtrIisisAreaMismatch	WA	gen	0	0
	2013	vRtrIisisRejectedAdjacency	WA	gen	0	0
	2014	vRtrIisisLSPTooLargeToPropagate	WA	gen	0	0
	2015	vRtrIisisOrigLSPBufSizeMismatch	WA	gen	0	0
	2016	vRtrIisisProtoSuppMismatch	WA	gen	0	0
	2017	vRtrIisisAdjacencyChange	WA	gen	0	0
	2018	vRtrIisisCircIdExhausted	WA	gen	0	0
	2019	vRtrIisisAdjRestartStatusChange	WA	gen	0	0
	2020	vRtrIisisLdpSyncTimerStarted	WA	gen	0	0
	2021	vRtrIisisLdpSyncExit	WA	gen	0	0
LAG:						
	2001	DynamicCostOn	WA	gen	0	0
	2002	DynamicCostOff	WA	gen	0	0
	2003	LagPortAddFailed	WA	gen	0	0
	2004	LagSubGroupSelected	WA	gen	0	0
	2005	LagPortAddFailureCleared	WA	gen	0	0
LDP:						
	2001	vRtrLdpStateChange	MI	gen	0	0
	2002	vRtrLdpInstanceStateChange	MI	gen	0	0
	2003	vRtrLdpIfStateChange	MI	sup	0	0
	2004	vRtrLdpGroupIdMismatch	MI	gen	0	0
LLDP:						
	2001	lldpRemTablesChange	MI	gen	0	0
LOGGER:						
L	2001	STARTED	MI	gen	5	0
	2002	tmnxLogTraceError	CR	gen	0	0
	2005	tmnxLogSpaceContention	MA	gen	0	0
	2006	tmnxLogAdminLocFailed	MA	gen	0	0
	2007	tmnxLogBackupLocFailed	MA	gen	0	0
	2008	tmnxLogFileRollover	MA	gen	0	0
	2009	tmnxLogFileDeleted	MI	gen	0	0
	2010	tmnxClear	IN	gen	0	0
	2011	tmnxTestEvent	IN	gen	0	0
	2012	tmnxLogEventThrottled	MA	gen	0	0
	2013	tmnxSysLogTargetProblem	MA	gen	0	0
	2014	tmnxLogAccountingDataLoss	MA	gen	0	0
	2015	tmnxStdEventsReplayed	MA	gen	0	0
L	2016	tmnxLogOnlyEventThrottled	MA	gen	0	0
MC_REDUNDANCY:						
	2001	tmnxMcRedundancyPeerStateChanged	WA	gen	0	0
	2002	tmnxMcRedundancyMismatchDetected	WA	gen	0	0
	2003	tmnxMcRedundancyMismatchResolved	WA	gen	0	0
	2004	tmnxMcPeerSyncStatusChanged	WA	gen	0	0

Show Commands

2005	tmnxMcSyncClientAlarmRaised	WA	gen	0	0
2006	tmnxMcSyncClientAlarmCleared	WA	gen	0	0
2007	tmnxSrrpSubnetMismatch	WA	gen	0	0
2008	tmnxSrrpSubnetMismatchCleared	WA	gen	0	0
2009	tmnxSrrpInstanceIdMismatch	WA	gen	0	0
2010	tmnxSrrpSapMismatch	WA	gen	0	0
2011	tmnxSrrpSapTagMismatch	WA	gen	0	0
2012	tmnxSrrpRedIfMismatch	WA	gen	0	0
2013	tmnxSrrpDualMaster	WA	gen	0	0
2014	tmnxMcLagInfoLagChanged	WA	gen	0	0
2015	tmnxSrrpSystemIpNotSet	WA	gen	0	0
2016	tmnxMcRingOperStateChanged	WA	gen	0	0
2017	tmnxMcRingInbCtrlOperStateChgd	WA	gen	0	0
2018	tmnxMcRingNodeLocOperStateChgd	WA	gen	0	0
2019	tmnxMcSyncClockSkewRaised	WA	gen	0	0
2020	tmnxMcSyncClockSkewCleared	WA	gen	0	0
2021	tmnxSrrpDuplicateSubIfAddress	WA	gen	0	0
2022	tmnxMcPeerRingsOperStateChanged	WA	gen	0	0
2023	tmnxSrrpTrapNewMaster	MI	gen	0	0
2024	tmnxSrrpBecameBackup	MI	gen	0	0
L 2025	srrpPacketDiscarded	MI	gen	0	0
2026	tmnxSrrpBfdIntfSessStateChgd	MI	gen	0	0
2027	tmnxMcPeerEPBfdSessionOpen	WA	gen	0	0
2028	tmnxMcPeerEPBfdSessionClose	WA	gen	0	0
2029	tmnxMcPeerEPBfdSessionUp	WA	gen	0	0
2030	tmnxMcPeerEPBfdSessionDown	WA	gen	0	0
2031	tmnxMcPeerEPOperDown	WA	gen	0	0
2032	tmnxMcPeerEPOperUp	WA	gen	0	0
2033	tmnxMCEPSessionPsvModeEnabled	WA	gen	0	0
2034	tmnxMCEPSessionPsvModeDisabled	WA	gen	0	0
MIRROR:					
2001	sourceEnabled	MI	gen	0	0
2002	sourceDisabled	MI	gen	0	0
2003	destinationEnabled	MI	gen	0	0
2004	destinationDisabled	MI	gen	0	0
2006	sourceIpFilterChange	MI	gen	0	0
2007	sourceMacFilterChange	MI	gen	0	0
2008	sourceSapChange	MI	gen	0	0
2009	sourceSubscriberChange	MI	gen	0	0
MPLS:					
2001	mplsXCUp	WA	gen	0	0
2002	mplsXCDown	WA	gen	0	0
2003	mplsTunnelUp	WA	gen	0	0
2004	mplsTunnelDown	WA	gen	0	0
2005	mplsTunnelRerouted	WA	sup	0	0
2006	mplsTunnelReoptimized	WA	sup	0	0
2007	vRtrMplsStateChange	WA	gen	0	0
2008	vRtrMplsIfStateChange	WA	gen	0	0
2009	vRtrMplsLspUp	WA	gen	0	0
2010	vRtrMplsLspDown	WA	gen	0	0
2011	vRtrMplsLspPathUp	WA	gen	0	0
2012	vRtrMplsLspPathDown	WA	gen	0	0
2013	vRtrMplsLspPathRerouted	WA	gen	0	0
2014	vRtrMplsLspPathResignaled	WA	gen	0	0
2015	vRtrMplsP2mpInstanceUp	WA	gen	0	0
2016	vRtrMplsP2mpInstanceDown	WA	gen	0	0
2017	vRtrMplsS2lSubLspUp	WA	gen	0	0
2018	vRtrMplsS2lSubLspDown	WA	gen	0	0
2019	vRtrMplsS2lSubLspRerouted	WA	gen	0	0
2020	vRtrMplsS2lSubLspResignaled	WA	gen	0	0
2021	vRtrMplsLspPathSoftPreempted	WA	gen	0	0

	2022	vRtrMplsLspPathLstFillReoptElig	WA	gen	0	0
	2023	vRtrMplsP2mpInstanceResignaled	WA	gen	0	0
	2024	vRtrMplsResignalTimerExpired	WA	gen	0	0
NTP:						
	2001	tmnxNtpAuthMismatch	WA	gen	0	0
	2002	tmnxNtpNoServersAvail	MA	gen	0	0
	2003	tmnxNtpServersAvail	MI	gen	0	0
	2008	tmnxNtpOperChange	WA	gen	0	0
	2009	tmnxNtpServerChange	MI	gen	0	0
OAM:						
	2001	tmnxOamPingProbeFailedV3	MI	gen	0	0
	2002	tmnxOamPingTestFailedV3	MI	gen	0	0
	2003	tmnxOamPingTestCompletedV3	MI	gen	0	0
	2004	tmnxAncpLoopbackTestCompleted	WA	gen	0	0
L	2005	tmnxAncpLoopbackTestCompletedL	WA	gen	0	0
	2050	tmnxOamTrPathChange	MI	gen	0	0
	2051	tmnxOamTrTestFailed	MI	gen	0	0
	2052	tmnxOamTrTestCompleted	MI	gen	0	0
L	2053	svcIdInvalid	MI	gen	0	0
L	2054	svcIdWrongType	MI	gen	0	0
	2055	tmnxOamLdpTttraceAutoDiscState	MI	gen	0	0
	2056	tmnxOamLdpTttraceFecProbeState	MI	gen	0	0
	2057	tmnxOamLdpTttraceFecDisStatus	MI	gen	0	0
	2101	tmnxOamSaaThreshold	MI	gen	0	0
OSPF:						
	2001	tmnxOspfVirtIfStateChange	WA	gen	0	0
	2002	tmnxOspfNbrStateChange	WA	gen	0	0
	2003	tmnxOspfVirtNbrStateChange	WA	gen	0	0
	2004	tmnxOspfIfConfigError	WA	gen	0	0
	2005	tmnxOspfVirtIfConfigError	WA	gen	0	0
	2006	tmnxOspfIfAuthFailure	WA	gen	0	0
	2007	tmnxOspfVirtIfAuthFailure	WA	gen	0	0
	2008	tmnxOspfIfRxBadPacket	WA	gen	0	0
	2009	tmnxOspfVirtIfRxBadPacket	WA	gen	0	0
	2010	tmnxOspfTxRetransmit	WA	sup	0	0
	2011	tmnxOspfVirtIfTxRetransmit	WA	sup	0	0
	2012	tmnxOspfAreaOriginateLsa	WA	sup	0	0
	2013	tmnxOspfAreaMaxAgeLsa	WA	gen	0	0
	2014	tmnxOspfLsdbOverflow	WA	gen	0	0
	2015	tmnxOspfLsdbApproachingOverflow	WA	gen	0	0
	2016	tmnxOspfIfStateChange	WA	gen	0	0
	2017	tmnxOspfNssaTranslatorStatusChg	WA	gen	0	0
	2018	tmnxOspfRestartStatusChange	WA	gen	0	0
	2019	tmnxOspfNbrRestartHlprStsChg	WA	gen	0	0
	2020	tmnxOspfVirtNbrRestartHlprStsChg	WA	gen	0	0
	2021	tmnxOspfSpfRunsStopped	WA	gen	0	0
	2022	tmnxOspfSpfRunsRestarted	WA	gen	0	0
	2023	tmnxOspfOverloadEntered	WA	gen	0	0
	2024	tmnxOspfOverloadExited	WA	gen	0	0
	2025	tmnxOspfAsOriginateLsa	WA	sup	0	0
	2026	tmnxOspfAsMaxAgeLsa	WA	gen	0	0
	2027	tmnxOspfLinkOriginateLsa	WA	sup	0	0
	2028	tmnxOspfLinkMaxAgeLsa	WA	gen	0	0
	2029	tmnxOspfLdpSyncTimerStarted	WA	gen	0	0
	2030	tmnxOspfLdpSyncExit	WA	gen	0	0
	2031	tmnxOspfShamIfStateChange	WA	gen	0	0
	2032	tmnxOspfShamNbrStateChange	WA	gen	0	0
	2033	tmnxOspfShamIfConfigError	WA	gen	0	0
	2034	tmnxOspfShamIfAuthFailure	WA	gen	0	0

Show Commands

```

2035 tmnxOspfShamIfRxBadPacket      WA gen      0      0
2036 tmnxOspfShamIfTxRetransmit     WA gen      0      0
2037 tmnxOspfShamNbrRestartHlprStsChg WA gen      0      0
2038 tmnxOspfFailureDisabled        WA gen      0      0
PORT:
2001 sonetSDHAlarmSet              MI gen      0      0
2002 sonetSDHAlarmClear            MI gen      0      0
2003 sonetSDHChannelAlarmSet       MI gen      0      0
2004 sonetSDHChannelAlarmClear     MI gen      0      0
2005 SFPInserted                    MI gen     17      0
2006 SFPRemoved                     MI gen      3      0
2008 SFPStatusFailure              MI gen      0      0
2009 portError                      MI gen      0      0
2010 yellowDiffDelayExceeded        MI gen      0      0
2011 redDiffDelayExceeded           MA gen      0      0
2012 bndlBadEndPtDiscriminator      MI gen      0      0
2013 ds3AlarmSet                   MI gen      0      0
2014 ds3AlarmClear                 MI gen      0      0
2015 dslAlarmSet                   MI gen      0      0
2016 dslAlarmClear                 MI gen      0      0
2017 etherAlarmSet                  MI gen      5      0
2018 etherAlarmClear               MI gen      4      0
2019 dslLoopbackStart              MI gen      0      0
2020 dslLoopbackStop               MI gen      0      0
2021 ds3LoopbackStart              MI gen      0      0
2022 ds3LoopbackStop               MI gen      0      0
2023 sdhLoopbackStart              MI gen      0      0
2024 sdhLoopbackStop               MI gen      0      0
2025 etherLoopDetected              MI gen      0      0
2026 etherLoopCleared              MI gen      0      0
2027 etherSpeedNotCompatible        MA gen      0      0
2028 etherDuplexNotCompatible       MA gen      0      0
2029 etherIngressRateCfgNotCompatible MA gen      0      0
2030 digitalDiagnosticMonitorFailed  MI gen      9      0
2031 SFPStatusDDMCorrupt            MI gen      0      0
2032 SFPStatusReadError             MI gen      0      0
2033 SFPStatusUnsupported           MI gen      0      0
2034 dsxClockSyncStateChange        MI gen      0      0
2035 bundleMlfrMemberLoopback       MI gen      0      0
2036 tmnxPortUnsupportedFunction     WA gen      0      0
2037 otuAlarms                      MI gen      0      0
ROUTE_POLICY:
L 2001 trigPolicyPrevEval           WA gen      0      0
RSVP:
2001 vRtrRsvpStateChange           WA gen      0      0
2002 vRtrRsvpIfStateChange         WA gen      0      0
2003 vRtrRsvpIfNbrStateUp          WA gen      0      0
2004 vRtrRsvpIfNbrStateDown        WA gen      0      0
SECURITY:
L 2001 cli_user_login              MI gen      3      0
L 2002 cli_user_logout             MI gen      2      0
L 2003 cli_user_login_failed        MI gen      0      0
L 2004 cli_user_login_max_attempts  MI gen      0      0
L 2005 ftp_user_login              MI gen      0      0
L 2006 ftp_user_logout              MI gen      0      0
L 2007 ftp_user_login_failed        MI gen      0      0
L 2008 ftp_user_login_max_attempts  MI gen      0      0
L 2009 ssh_user_login               MI gen      0      0
L 2010 ssh_user_logout              MI gen      0      0
L 2011 ssh_user_login_failed        MI gen      0      0
L 2012 ssh_user_login_max_attempts  MI gen      0      0

```

	2014	radiusOperStatusChange	MI	gen	0	0
L	2015	user_disconnect	MA	gen	0	0
L	2016	radiusSystemIpAddrNotSet	MA	gen	0	0
	2018	tacplusOperStatusChange	MI	gen	0	0
L	2019	mafEntryMatch	MA	gen	0	0
L	2020	ftp_transfer_successful	MI	gen	0	0
L	2021	ftp_transfer_failed	MI	gen	0	0
L	2022	enable_admin	WA	gen	0	0
L	2023	host_snmp_attempts	WA	gen	0	0
	2024	SSH_server_preserve_key_fail	MI	gen	0	0
	2025	tacplusInetSrvrOperStatusChange	MI	gen	0	0
	2026	radiusInetServerOperStatusChange	MI	gen	0	0
	2027	tmnxKeyChainAuthFailure	MI	gen	0	0
	2028	tmnxCpmProtViolPort	WA	gen	0	0
	2029	tmnxCpmProtViolPortAgg	WA	gen	0	0
	2030	tmnxCpmProtViolIf	WA	gen	0	0
	2031	tmnxCpmProtViolSap	WA	gen	0	0
	2032	tmnxCpmProtViolMac	WA	gen	0	0
	2033	tmnxCpmProtViolVdoSvcClient	WA	gen	0	0
	2034	tmnxCpmProtViolVdoVrtrClient	WA	gen	0	0
	2206	tmnxConfigModify	WA	gen	2	0
	2207	tmnxConfigCreate	WA	gen	2	0
	2208	tmnxConfigDelete	WA	gen	0	0
	2209	tmnxStateChange	WA	gen	0	0
SNMP:						
	2001	coldStart	MA	gen	1	0
	2002	warmStart	MA	gen	0	0
	2003	authenticationFailure	MI	sup	0	0
	2004	linkDown	WA	gen	5	0
	2005	linkUp	WA	gen	8	0
	2101	risingAlarm	MA	gen	0	0
	2102	fallingAlarm	MA	gen	0	0
	2201	snmpdError	MA	gen	0	0
STP:						
	2001	topologyChangeSapMajorState	WA	gen	0	0
	2002	newRootSap	WA	gen	0	0
	2003	topologyChangeVcpState	WA	gen	0	0
	2004	newRootVcpState	WA	gen	0	0
	2005	topologyChangeSapState	WA	gen	0	0
	2006	receivedTCN	WA	gen	0	0
	2007	newRootBridge	WA	gen	0	0
	2008	unacknowledgedTCN	WA	gen	0	0
	2009	higherPriorityBridge	WA	gen	0	0
	2011	sapEncapPVST	MI	gen	0	0
	2012	sapEncapDot1d	MI	gen	0	0
	2014	tmnxSvcTopoChgSdpBindMajorState	WA	gen	0	0
	2015	tmnxSvcNewRootSdpBind	WA	gen	0	0
	2016	tmnxSvcTopoChgSdpBindState	WA	gen	0	0
	2017	tmnxSvcSdpBindRcvdTCN	WA	gen	0	0
	2018	tmnxSvcSdpBindRcvdHigherBriPrio	WA	gen	0	0
	2019	tmnxSvcSdpBindEncapPVST	MI	gen	0	0
	2020	tmnxSvcSdpBindEncapDot1d	MI	gen	0	0
	2021	tmnxNewCistRegionalRootBridge	WA	gen	0	0
	2022	tmnxNewMstiRegionalRootBridge	WA	gen	0	0
	2023	tmnxStpRootGuardViolation	WA	gen	0	0
	2024	tmnxStpMeshNotInMstRegion	WA	gen	0	0
	2025	tmnxSapStpExcepCondStateChng	WA	gen	0	0
	2026	tmnxSdpBndStpExcepCondStateChng	WA	gen	0	0
	2050	sapActiveProtocolChange	MI	gen	0	0

Show Commands

2051	tmnxSvcSdpActiveProtocolChange	MI	gen	0	0
2052	vcpActiveProtocolChange	MI	gen	0	0
2053	topologyChangePipMajorState	WA	gen	0	0
2054	topologyChangePipState	WA	gen	0	0
2055	tmnxPipStpExcepCondStateChng	WA	gen	0	0
2056	pipActiveProtocolChange	MI	gen	0	0
SVCMMGR:					
2011	svcTlsMacPinningViolation	WA	gen	0	0
2103	svcStatusChanged	MI	gen	4	0
2104	svcTlsFdbTableFullAlarmRaised	MI	gen	0	0
2105	svcTlsFdbTableFullAlarmCleared	MI	gen	0	0
2108	iesIfStatusChanged	MI	gen	0	0
2109	tmnxSvcObjTodSuiteApplicFailed	WA	gen	0	0
2110	tmnxEndPointTxActiveChanged	WA	gen	0	0
2111	tmnxSvcPEDiscPolServOperStatChg	MI	gen	0	0
2120	svcTlsMrpAttrRegistrationFailed	MI	gen	0	0
2125	svcTlsMrpAttrTblFullAlarmRaised	MI	gen	0	0
2126	svcTlsMrpAttrTblFullAlarmCleared	MI	gen	0	0
2128	svcEpipePbbOperStatusChanged	MI	gen	0	0
2203	sapStatusChanged	MI	gen	2	0
2204	sapTlsMacAddrLimitAlarmRaised	MI	gen	0	0
2205	sapTlsMacAddrLimitAlarmCleared	MI	gen	0	0
2206	hostConnectivityLost	WA	gen	0	0
2207	hostConnectivityRestored	WA	gen	0	0
2208	sapReceivedProtSrcMac	MI	gen	0	0
2209	sapTlsMacMoveExceeded	MI	gen	0	0
2210	sapPortStateChangeProcessed	MA	gen	0	0
2211	sapCemPacketDefectAlarm	MI	gen	0	0
2212	sapCemPacketDefectAlarmClear	MI	gen	0	0
2213	msapStateChanged	MI	gen	0	0
2214	msapCreationFailure	MI	gen	0	0
2303	sdpStatusChanged	MI	gen	0	0
2306	sdpBindStatusChanged	MI	gen	0	0
L 2307	sdpKeepAliveStarted	MI	gen	0	0
L 2308	sdpKeepAliveStopped	MI	gen	0	0
L 2309	sdpKeepAliveProbeFailure	MI	gen	0	0
L 2310	sdpKeepAliveLateReply	MI	gen	0	0
2311	sdpTlsMacAddrLimitAlarmRaised	MI	gen	0	0
2312	sdpTlsMacAddrLimitAlarmCleared	MI	gen	0	0
2313	sdpBindPwPeerStatusBitsChanged	MI	gen	0	0
2314	sdpBindTlsMacMoveExceeded	MI	gen	0	0
2315	sdpBindPwPeerFaultAddrChanged	MI	gen	0	0
2316	sdpBindSdpStateChangeProcessed	MA	gen	0	0
2317	sdpBandwidthOverbooked	MA	gen	0	0
2318	sdpBindInsufficientBandwidth	MA	gen	0	0
2319	dynamicSdpConfigChanged	MA	gen	0	0
2320	dynamicSdpBindConfigChanged	MA	gen	0	0
2321	dynamicSdpCreationFailed	MA	gen	0	0
2322	dynamicSdpBindCreationFailed	MA	gen	0	0
2401	svcTlsMfibTableFullAlarmRaised	MI	gen	0	0
2402	svcTlsMfibTableFullAlarmCleared	MI	gen	0	0
2500	tmnxSubscriberCreated	WA	gen	0	0
2501	tmnxSubscriberDeleted	WA	gen	0	0
2502	tmnxSubscriberRenamed	WA	gen	0	0
2503	tmnxSubAcctPlcyFailure	WA	gen	0	0
2504	tmnxSubMcsRelatedProblem	WA	gen	0	0
2505	tmnxSubAuthPlcyRadSerOperStatChg	MI	gen	0	0
2506	tmnxSubAcctPlcyRadSerOperStatChg	MI	gen	0	0
2507	svcEndPointMacLimitAlarmRaised	MI	gen	0	0
2508	svcEndPointMacLimitAlarmCleared	MI	gen	0	0
2509	tmnxSubRadSapDisconnectError	WA	gen	0	0

2510	tmnxSubRadSdpBndDisconnectError	WA	gen	0	0
2511	tmnxSubRadSapCoAError	WA	gen	0	0
2512	tmnxSubRadSdpBndCoAError	WA	gen	0	0
2513	tmnxSubRadSapSubAuthError	WA	gen	0	0
2514	tmnxSubRadSdpBndSubAuthError	WA	gen	0	0
2515	svcFdbMimDestTblFullAlarm	MI	gen	0	0
2516	svcFdbMimDestTblFullAlarmCleared	MI	gen	0	0
2517	svcPersistencyProblem	WA	gen	0	0
2520	svcArpHostPopulateErr	WA	gen	0	0
2522	svcEPMCEPConfigMismatch	WA	gen	0	0
2523	svcEPMCEPConfigMismatchResolved	WA	gen	0	0
2524	svcEPMCEPPassiveModeActive	WA	gen	0	0
2525	svcEPMCEPPassiveModePassive	WA	gen	0	0
2526	sapHostBGPPeeringSetupFailed	MI	gen	0	0
2527	tmnxSubUserCategoryOutOfCredit	MI	gen	0	0
2528	svcRestoreHostProblem	WA	gen	0	0
2529	tmnxSubUserCategoryRefreshCredit	MI	gen	0	0
2530	tmnxSubUserCategoryError	MI	gen	0	0
SYSTEM:					
2001	stiDateAndTimeChanged	WA	gen	0	0
2002	ssiSaveConfigSucceeded	MA	gen	0	0
2003	ssiSaveConfigFailed	CR	gen	0	0
2004	sbiBootConfig	MA	gen	1	0
2005	sbiBootSnmpd	MA	gen	1	0
2006	tmnxConfigModify	WA	gen	66	0
2007	tmnxConfigCreate	WA	gen	11	0
2008	tmnxConfigDelete	WA	gen	0	0
2009	tmnxStateChange	WA	gen	7	0
2010	tmnxModuleMallocFailed	MA	gen	0	0
2011	tmnxTrapDropped	MA	gen	0	0
2012	ssiSyncConfigOK	WA	gen	0	0
2013	ssiSyncConfigFailed	CR	gen	0	0
2014	ssiSyncBootEnvOK	WA	gen	0	0
2015	ssiSyncBootEnvFailed	CR	gen	0	0
L 2016	socket_bind_failed	CR	gen	0	0
L 2017	socket_conn_accept_failed	CR	gen	0	0
2018	sntpTimeDiffExceedsThreshold	MA	gen	0	0
2022	tmnxSssiMismatch	MA	gen	0	0
2023	tmnxSnmpdStateChange	MA	gen	1	0
2024	tmnxRedStandbySyncing	MA	gen	0	0
2025	tmnxRedStandbyReady	MA	gen	0	0
2026	tmnxRedStandbySyncLost	CR	gen	0	0
2027	tmnxRedSwitchover	CR	gen	0	0
2028	tmnxRedCpmActive	CR	gen	0	0
2029	tmnxRedSingleCpm	CR	gen	0	0
2030	persistencyClosedAlarmRaised	MA	gen	0	0
2031	persistencyClosedAlarmCleared	MA	gen	0	0
2032	tmnxSntpOperChange	MA	gen	0	0
2034	tmnxFtpClientFailure	MI	gen	0	0
2037	persistencyEventReport	WA	gen	0	0
2038	sbiBootConfigFailFileError	MA	gen	0	0
2039	sbiBootConfigOKFileError	MA	gen	0	0
2101	schedActionFailure	MA	gen	0	0
2102	smScriptAbort	MA	gen	0	0
2103	smScriptResult	MI	sup	0	0
2104	smScriptException	MI	sup	0	0
USER:					
L 2001	cli_user_login	MI	gen	3	0
L 2002	cli_user_logout	MI	gen	2	0

Show Commands

```

L 2003 cli_user_login_failed           MI gen           0           0
L 2004 cli_user_login_max_attempts     MI gen           0           0
L 2005 ftp_user_login                  MI gen           0           0
L 2006 ftp_user_logout                 MI gen           0           0
L 2007 ftp_user_login_failed           MI gen           0           0
L 2008 ftp_user_login_max_attempts     MI gen           0           0
L 2009 cli_user_io                     MI sup          0           35
L 2010 snmp_user_set                   MI sup          0           0
L 2011 cli_config_io                   MI gen          276          0
VRTR:
  2001 tmnxVRtrMidRouteTCA             MI gen           0           0
  2002 tmnxVRtrHighRouteTCA            MI gen           0           0
  2003 tmnxVRtrHighRouteCleared        MI gen           0           0
  2004 tmnxVRtrIllegalLabelTCA        MA gen           0           0
  2008 tmnxVRtrMaxArpEntriesTCA        MA gen           0           0
  2009 tmnxVRtrMaxArpEntriesCleared    MI gen           0           0
  2011 tmnxVRtrMaxRoutes                MI gen           0           0
  2012 tmnxVRtrBfdSessionDown          MA gen           0           0
  2013 tmnxVRtrBfdMaxSessionOnSlot     MA gen           0           0
  2014 tmnxVRtrBfdPortTypeNotSupported MA gen           0           0
  2015 tmnxVRtrBfdSessionUp            MA gen           0           0
  2016 tmnxVRtrIPv6MidRouteTCA         MI gen           0           0
  2017 tmnxVRtrIPv6HighRouteTCA        MI gen           0           0
  2018 tmnxVRtrIPv6HighRouteCleared    MI gen           0           0
  2019 tmnxVRtrStaticRouteCPEStatus    MI gen           0           0
  2020 tmnxVRtrBfdSessionDeleted        MI gen           0           0
  2021 tmnxVRtrBfdSessionProtChange    MI gen           0           0
  2022 tmnxVRtrManagedRouteAddFailed   MI gen           0           0
  2023 tmnxVRtrFibOccupancyThreshold    MI sup           0           0
  2024 tmnxVRtrInetAddressAttachFailed  MI gen           0           0
  2029 tmnxVRtrIfLdpSyncTimerStart     WA sup           0           0
  2030 tmnxVRtrIfLdpSyncTimerStop      WA sup           0           0
=====

```

A:ALA-1# show log event-control ospf

=====
Log Events
=====

Application

ID#	Event Name	P	g/s	Logged	Dropped
2001	ospfVirtIfStateChange	WA	gen	0	0
2002	ospfNbrStateChange	WA	gen	1	0
2003	ospfVirtNbrStateChange	WA	gen	0	0
2004	ospfIfConfigError	WA	gen	0	0
2005	ospfVirtIfConfigError	WA	gen	0	0
2006	ospfIfAuthFailure	WA	gen	0	0
2007	ospfVirtIfAuthFailure	WA	gen	0	0
2008	ospfIfRxBadPacket	WA	gen	0	0
2009	ospfVirtIfRxBadPacket	WA	gen	0	0
2010	ospfTxRetransmit	WA	sup	0	0
2011	ospfVirtIfTxRetransmit	WA	sup	0	0
2012	ospfOriginateLsa	WA	sup	0	404
2013	ospfMaxAgeLsa	WA	gen	3	0
2014	ospfLsdbOverflow	WA	gen	0	0
2015	ospfLsdbApproachingOverflow	WA	gen	0	0
2016	ospfIfStateChange	WA	gen	2	0
2017	ospfNssaTranslatorStatusChange	WA	gen	0	0
2018	vRtrOspfSpfRunsStopped	WA	gen	0	0
2019	vRtrOspfSpfRunsRestarted	WA	gen	0	0
2020	vRtrOspfOverloadEntered	WA	gen	1	0

```

2021 vRtrOspfOverloadExited          WA gen          0          0
2022 ospfRestartStatusChange         WA gen          0          0
2023 ospfNbrRestartHelperStatusChange WA gen          0          0
2024 ospfVirtNbrRestartHelperStsChg  WA gen          0          0
=====
A:ALA-1#

A:ALA-1# show log event-control ospf ospfVirtIfStateChange
=====
Log Events
=====
Application
ID#      Event Name                      P   g/s      Logged      Dropped
-----
2001 ospfVirtIfStateChange        WA  gen          0          0
=====
A:ALA-1#

```

file-id

- Syntax** `file-id [log-file-id]`
- Context** `show>log`
- Description** This command displays event file log information.
If no command line parameters are specified, a summary output of all event log files is displayed. Specifying a file ID displays detailed information on the event file log.
- Parameters** *log-file-id* — Displays detailed information on the specified event file log.
Values 1 up to 99
- Output** **Log File Output** — The following table describes the output fields for a log file summary.

Label	Description
file-id	The log file ID.
rollover	The rollover time for the log file which is how long in between partitioning of the file into a new file.
retention	The retention time for the file in the system which is how long the file should be retained in the file system.
admin location	The primary flash device specified for the file location. none — indicates no specific flash device was specified.
oper location	The actual flash device on which the log file exists.
file-id	The log file ID.

Label	Description (Continued)
rollover	The rollover time for the log file which is how long in between partitioning of the file into a new file.
retention	The retention time for the file in the system which is how long the file should be retained in the file system.
file name	The complete pathname of the file associated with the log ID.
expired	Indicates whether or not the retention period for this file has passed.
state	in progress – Indicates the current open log file. complete – Indicates the old log file.

```
*A:MTUSN945189# show log file-id
=====
File Id List
=====
file-id  rollover  retention  admin      backup      oper
          location   location   location
-----
1         30         500       cf1:       none        cf1:
2         30         500       cf1:       none        cf1:
3         30         500       cf1:       none        cf1:
4         30         500       cf1:       none        cf1:
5         30         500       cf1:       none        cf1:
6         30         500       cf1:       none        cf1:
7         30         500       cf1:       none        cf1:
8         30         500       cf1:       none        cf1:
9         30         500       cf1:       none        cf1:
10        30         500       cf1:       none        cf1:
11        30         500       cf1:       none        cf1:
12        30         500       cf1:       none        cf1:
13        30         500       cf1:       none        cf1:
14        30         500       cf1:       none        cf1:
15        30         500       cf1:       none        cf1:
16        30         500       cf1:       none        cf1:
17        30         500       cf1:       none        cf1:
18        30         500       cf1:       none        cf1:
=====
*A:MTUSN945189#
```

```
A:MTUSN945189# show log file-id 1
=====
File Id List
=====
file-id  rollover  retention  admin      backup      oper
          location   location   location
-----
1         2800      500       cf1:       none        cf1:
=====
File Id 1  Location cf1:
=====
file name                               expired  state
-----
```

```
cf1:\act\act0101-20010518-085306.xml.gz no complete
=====
*A:MTUSN945189#
```

filter-id

- Syntax** `filter-id [filter-id]`
- Context** `show>log`
- Description** This command displays event log filter policy information.
- Parameters** *filter-id* — Displays detailed information on the specified event filter policy ID.
- Values** 1 up to 65535
- Output** **Event Log Filter Summary Output** — The following table describes the output fields for event log filter summary information.

Table 36: Event Log Filter Summary Output Fields

Label	Description
Filter Id	The event log filter ID.
Applied	no. The event log filter is not currently in use by a log ID. yes. The event log filter is currently in use by a log ID.
Default Action	drop. The default action for the event log filter is to drop events not matching filter entries. forward. The default action for the event log filter is to forward events not matching filter entries.
Description	The description string for the filter ID.

Sample Output

```
*A:ALA-48>config>log# show log filter-id
=====
Log Filters
=====
Filter Applied Default Description
Id           Action
-----
1           no           forward
5           no           forward
10          no           forward
1001        yes          drop          Collect events for Serious Errors Log
=====
*A:ALA-48>config>log#
```

Event Log Filter Detailed Output — The following table describes the output fields for detailed event log filter information.

Table 37: Event Log Filter Detail Output Fields

Label	Description
Filter-id	The event log filter ID.
Applied	no — The event log filter is not currently in use by a log ID. yes — The event log filter is currently in use by a log ID.
Default Action	drop — The default action for the event log filter is to drop events not matching filter entries. forward — The default action for the event log filter is to forward events not matching filter entries.
Description (Filter-id)	The description string for the filter ID.

Table 38: Log Filter Match Criteria Output Fields

Label	Description
Entry-id	The event log filter entry ID.
Action	default — There is no explicit action for the event log filter entry and the filter’s default action is used on matching events. drop — The action for the event log filter entry is to drop matching events. forward — The action for the event log filter entry is to forward matching events.
Description (Entry-id)	The description string for the event log filter entry.
Application	The event log filter entry application match criterion.
Event Number	The event log filter entry application event ID match criterion.
Severity	cleared — The log event filter entry application event severity cleared match criterion. indeterminate — The log event filter entry application event severity indeterminate match criterion. critical — The log event filter entry application event severity critical match criterion.

Table 38: Log Filter Match Criteria Output Fields (Continued)

Label	Description (Continued)
	major – The log event filter entry application event severity cleared match criterion.
	minor – The log event filter entry application event severity minor match criterion.
	warning – The log event filter entry application event severity warning match criterion.
Subject	Displays the event log filter entry application event ID subject string match criterion.
Router	Displays the event log filter entry application event ID router <i>router-instance</i> string match criterion.
Operator	There is an operator field for each match criteria: application, event number, severity, and subject.
	equal – Matches when equal to the match criterion.
	erThanOrEqual – Matches when greater than or equal to the match criterion.
	greaterThanOrEqual – Matches when greater than or equal to the match criterion.
	lessThan – Matches when less than the match criterion.
	lessThanOrEqual – Matches when less than or equal to the match criterion.
	notEqual – Matches when not equal to the match criterion.
	off – No operator specified for the match criterion.

Sample Output

```
*A:ALA-48>config>log# show log filter-id 1001
=====
Log Filter
=====
Filter-id      : 1001      Applied      : yes      Default Action: drop
Description    : Collect events for Serious Errors Log
-----
Log Filter Match Criteria
-----
Entry-id      : 10              Action       : forward
Application    :                  Operator     : off
Event Number   : 0              Operator     : off
Severity       : major          Operator     : greaterThanOrEqual
Subject       :                  Operator     : off
```

Show Commands

```

Match Type      : exact string
Router          :
Operator        : off
Match Type      : exact string
Description     : Collect only events of major severity or higher
-----
=====
*A:ALA-48>config>log#

```

log-collector

- Syntax** **log-collector**
- Context** show>log
- Description** Show log collector statistics for the main, security, change and debug log collectors.
- Output** **Log-Collector Output** — The following table describes log-collector output fields.

Table 39: Show Log-Collector Output Fields

Label	Description
<Collector Name>	<p>Main — The main event stream contains the events that are not explicitly directed to any other event stream.</p> <p>Security — The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted.</p> <p>Change — The change event stream contains all events that directly affect the configuration or operation of this node.</p> <p>Debug — The debug-trace stream contains all messages in the debug stream.</p>
Dest. Log ID	Specifies the event log stream destination.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Status	<p>Enabled — Logging is enabled.</p> <p>Disabled — Logging is disabled.</p>

Table 39: Show Log-Collector Output Fields (Continued)

Label	Description (Continued)
Dest. Type	<p>Console – A log created with the console type destination displays events to the physical console device.</p> <p>Events are displayed to the console screen whether a user is logged in to the console or not.</p> <p>A user logged in to the console device or connected to the CLI via a remote telnet or SSH session can also create a log with a destination type of 'session'. Events are displayed to the session device until the user logs off. When the user logs off, the 'session' type log is deleted.</p> <p>Syslog – All selected log events are sent to the syslog address.</p> <p>SNMP traps – Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables.</p> <p>File – All selected log events will be directed to a file on one of the compact flash disks.</p> <p>Memory – All selected log events will be directed to an in-memory storage area.</p>

Sample Output

```

A:ALA-1# show log log-collector
=====
Log Collectors
=====
Main          Logged   : 1224          Dropped   : 0
  Dest Log Id: 99   Filter Id: 0       Status: enabled   Dest Type: memory
  Dest Log Id: 100 Filter Id: 1001    Status: enabled   Dest Type: memory

Security      Logged   : 3           Dropped   : 0

Change       Logged   : 3896        Dropped   : 0

Debug        Logged   : 0           Dropped   : 0

=====
A:ALA-1#

```

log-id

Syntax	log-id [<i>log-id</i>] [severity <i>severity-level</i>] [application <i>application</i>] [sequence <i>from-seq</i> [<i>to-seq</i>]] [count <i>count</i>] [router <i>router-instance</i> [expression]] [subject <i>subject</i> [regexp]] [ascending descending]
Context	show>log
Description	<p>This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.</p> <p>If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.</p> <p>If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.</p> <p>Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.</p>
Parameters	<p><i>log-id</i> — Displays the contents of the specified file log or memory log ID. The log ID must have a destination of an SNMP or file log or a memory log for this parameter to be used.</p> <p>Default Displays the event log summary</p> <p>Values 1 — 99</p> <p>severity <i>severity-level</i> — Displays only events with the specified and higher severity.</p> <p>Default All severity levels</p> <p>Values cleared, indeterminate, critical, major, minor, warning</p> <p>application <i>application</i> — Displays only events generated by the specified application.</p> <p>Default All applications</p> <p>expression — Specifies to use a regular expression as match criteria for the router instance string.</p> <p>sequence <i>from-seq</i> [<i>to-seq</i>] — Displays the log entry numbers from a particular entry sequence number (<i>from-seq</i>) to another sequence number (<i>to-seq</i>). The <i>to-seq</i> value must be larger than the <i>from-seq</i> value.</p> <p>If the <i>to-seq</i> number is not provided, the log contents to the end of the log is displayed unless the count parameter is present in which case the number of entries displayed is limited by the count.</p> <p>Default All sequence numbers</p> <p>Values 1 — 4294967295</p> <p>count <i>count</i> — Limits the number of log entries displayed to the <i>number</i> specified.</p> <p>Default All log entries</p> <p>Values 1 — 4294967295</p> <p><i>router-instance</i> — Specifies a router name up to 32 characters to be used in the display criteria.</p> <p>subject <i>subject</i> — Displays only log entries matching the specified text <i>subject</i> string. The subject is the object affected by the event, for example the port-id would be the subject for a link-up or link-down event.</p>

regexp — Specifies to use a regular expression as parameters with the specified *subject* string..

ascending / descending — Specifies sort direction. Logs are normally shown from the newest entry to the oldest in **descending** sequence number order on the screen. When using the **ascending** parameter, the log will be shown from the oldest to the newest entry.

Default Descending

Output Show Log-ID Output — The following table describes the log ID field output.

Label	Description
Log Id	An event log destination.
Source	no — The event log filter is not currently in use by a log ID. yes — The event log filter is currently in use by a log ID.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Admin State	Up — Indicates that the administrative state is up. Down — Indicates that the administrative state is down.
Oper State	Up — Indicates that the operational state is up. Down — Indicates that the operational state is down.
Logged	The number of events that have been sent to the log source(s) that were forwarded to the log destination.
Dropped	The number of events that have been sent to the log source(s) that were not forwarded to the log destination because they were filtered out by the log filter.
Dest. Type	Console — All selected log events are directed to the system console. If the console is not connected, then all entries are dropped. Syslog — All selected log events are sent to the syslog address. SNMP traps — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables. File — All selected log events will be directed to a file on one of the compact flash disks. Memory — All selected log events will be directed to an in-memory storage area.
Dest ID	The event log stream destination.

Label	Description (Continued)
Size	The allocated memory size for the log.
Time format	The time format specifies the type of timestamp format for events sent to logs where log ID destination is either syslog or file. When the time format is UTC, timestamps are written using the Coordinated Universal Time value. When the time format is local, timestamps are written in the system's local time.

Sample Output

```
A:ALA-1# show log log-id
=====
Event Logs
=====
Log Source      Filter Admin Oper  Logged  Dropped Dest      Dest  Size
Id              Id      State State                    Type     Id
-----
1  none          none   up   down   52      0      file      10   N/A
2  C             none   up   up     41      0      syslog    1    N/A
99 M            none   up   up    2135   0      memory    500
=====
A:ALA-1#
```

Sample Memory or File Event Log Contents Output

```
A:gal171# show log log-id 99
=====
Event Log 99
=====
Description : Default System Log
Memory Log contents [size=500  next event=70  (not wrapped)]

69 2007/01/25 18:20:40.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

68 2007/01/25 17:48:38.16 UTC WARNING: SYSTEM #2006 Base LOGGER
"New event throttle interval 10, configuration modified"

67 2007/01/25 00:34:53.97 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

66 2007/01/24 22:59:22.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

65 2007/01/24 02:08:47.92 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."
...
=====
A:gal171
```

```

A:NS061550532>config>log>snmp-trap-group# show log log-id 1
=====
Event Log 1
=====
SNMP Log contents [size=100  next event=3  (not wrapped)]
Cannot send to SNMP target address 10.1.1.1.

14 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2007 Base VR 1:
"Instance is in administrative state: inService, operational state: inService"

13 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2008 Base VR 1:
"Interface linkToIxia is in administrative state: inService, operational state:
inService"
....
=====
A:NS061550532>config>log>snmp-trap-group#

```

snmp-trap-group

- Syntax** `snmp-trap-group [log-id]`
- Context** `show>log`
- Description** This command displays SNMP trap group configuration information.
- Parameters** *log-id* — Displays only SNMP trap group information for the specified trap group log ID.
- Values** 1 — 100
- Output** **SNMP Trap Group Output** — The following table describes SNMP trap group output fields.

Table 40: SNMP Trap Group Output Fields

Label	Description
Log-ID	The log destination ID for an event stream.
Address	The IP address of the trap receiver,
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are <code>snmpv1</code> , <code>snmpv2c</code> , <code>snmpv3</code> .
Community	The community string required by <code>snmpv1</code> or <code>snmpv2c</code> trap receivers.
Security-Level	The required authentication and privacy levels required to access the views on this node.

Sample SNMP Trap Group Output

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44
```

```

=====
SNMP Trap Group 44
=====
Description : none
-----
Name       : ntt-test
Address    : 10.10.10.3
Port      : 162
Version   : v2c
Community  : ntttesting
Sec. Level : none
-----
Name       : test2
Address    : 20.20.20.5
Port      : 162
Version   : v2c
Community  : ntttesting
Sec. Level : none
=====
A:SetupCLI>config>log>snmp-trap-group#

```

syslog

- Syntax** **syslog** [*syslog-id*]
- Context** show>log
- Description** This command displays syslog event log destination summary information or detailed information on a specific syslog destination.
- Parameters** *syslog-id* — Displays detailed information on the specified syslog event log destination.
 Values 1 — 10
- Output** **Syslog Event Log Destination Summary Output** — The following table describes the syslog output fields.

Table 41: Show Log Syslog Output Fields

Label	Description
Syslog ID	The syslog ID number for the syslog destination.
IP Address	The IP address of the syslog target host.
Port	The configured UDP port number used when sending syslog messages.
Facility	The facility code for messages sent to the syslog target host.
Severity Level	The syslog message severity level threshold.
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.

Table 41: Show Log Syslog Output Fields (Continued)

Label	Description
Prefix Present	Yes – A log prefix was prepended to the syslog message sent to the syslog host. No – A log prefix was not prepended to the syslog message sent to the syslog host.
Description	A text description stored in the configuration file for a configuration context.
LogPrefix	The prefix string prepended to the syslog message.
Log-id	Events are directed to this destination.

Sample Syslog Event Log Destination Summary Output

```
*A:ALA-48>config>log# show log syslog
=====
Syslog Target Hosts
=====
Id      Ip Address          Port      Sev Level
      Below Level Drop      Facility  Pfx Level
-----
2       unknown            514      info
      0                  local7    yes
3       unknown            514      info
      0                  local7    yes
5       unknown            514      info
      0                  local7    yes
10      unknown            514      info
      0                  local7    yes
=====
*A:ALA-48>config>log#

*A:MV-SR>config>log# show log syslog 1
=====
Syslog Target 1
=====
IP Address      : 192.168.15.22
Port            : 514
Log-ids         : none
Prefix          : Sr12
Facility        : local1
Severity Level  : info
Prefix Level    : yes
Below Level Drop : 0
Description     : Linux Station Springsteen
=====
*A:MV-SR>config>log#
```

Clear Commands

log

Syntax	log <i>log-id</i>
Context	clear
Description	<p>Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.</p> <p>This command is only applicable to event logs that are directed to file destinations and memory destinations.</p> <p>SNMP, syslog and console/session logs are not affected by this command.</p>
Parameters	<p><i>log-id</i>. The event log ID to be initialized/rolled over.</p> <p>Values 1 — 100</p>

Facility Alarms

In This Chapter

This chapter provides information about configuring event and accounting logs in the system.

Topics in this chapter include:

- [Facility Alarms Overview on page 378](#)
- [Facility Alarms vs. Log Events on page 379](#)
- [Facility Alarm Severities and Alarm LED Behavior on page 381](#)
- [Facility Alarm Hierarchy on page 422](#)
- [Facility Alarm Hierarchy on page 422](#)

Facility Alarms Overview

Facility Alarms provide a useful tool for operators to easily track and display the basic status of their equipment facilities.

CLI display (show routines) allows the system operator to easily identify current facility alarm conditions and recently cleared alarms without searching event logs or monitoring various card and port show commands to determine the health of managed objects in the system such as cards and ports.

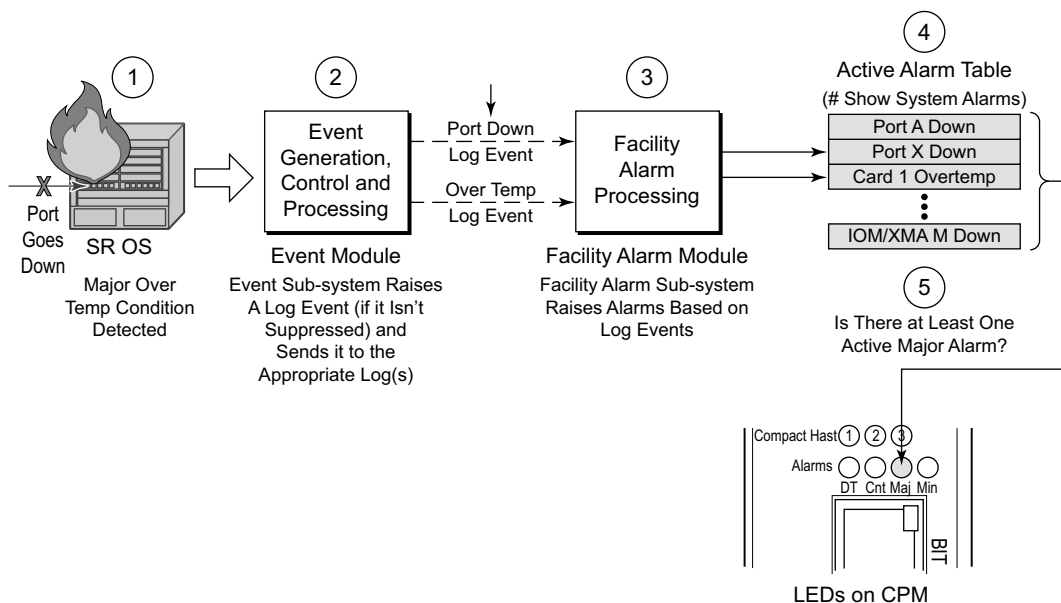
The 7210 SAS OS alarm model is based on RFC 3877, *Alarm Management Information Base (MIB)*, (which evolved from the IETF DISMAN drafts).

Facility Alarms vs. Log Events

Facility Alarms are different than (log) events. Events are a single point in time and are generally stateless. Facility Alarms have a state (at least two states: active and clear) and duration and can be modelled with state transition events (raised, cleared).

The Facility Alarms module processes log events in order to generate the raised and cleared state for the alarms. If a raising log event is suppressed under event-control, then the associated Alarm will not be raised. If a clearing log event is suppressed under event-control, then it is still processed for the purpose of clearing the associated alarm. Log event filtering, throttling and discarding of events during overload do not affect Facility Alarm processing. Log events are processed by the Facility Alarm module before they are discarded in all cases.

Figure 6 illustrates the relationship of log events, alarms and the LEDs.



OSSG651

Figure 6: Log Events, Alarms and LEDs

NOTE: Some of the 7210 platforms do not have Critical, Major, and Minor LEDs and Alarm Output PINs. On these platforms, an event is raised and only a log is generated.

Facility Alarms vs. Log Events

Facility Alarms are different and independent functionality from other uses of the term *alarm* in SR OS such as:

- **configure port ethernet report-alarm**
- **configure system thresholds no memory-use-alarm**
- **configure system thresholds rmon no alarm**

Facility Alarm Severities and Alarm LED Behavior

The Alarm LEDs on the CPM/CCM reflects the current status of the Facility Alarms:

- The Critical Alarm LED (if available on the 7210 SAS platform), is lit if there is 1 or more active Critical Facility Alarms.
- Similarly with the Major and Minor alarm LEDs (if available on the 7210 SAS platform).
- The OT Alarm LED (if available on the 7210 SAS platform), is not controlled by the Facility Alarm module.

The supported alarm severities are as follows:

- Critical (with an associated LED)
- Major (with an associated LED)
- Minor (with an associated LED)
- Warning (no LED)

Alarms inherit their severity from the raising event.

Log events that are a raising event for a facility alarm configured with a severity of *indeterminate* or *cleared* will result in those alarms not being raised (but clearing events are processed in order to clear alarms regardless of the severity of the clearing event).

Changing the severity of a raising event only affects subsequent occurrences of that event and alarms. Alarms that are already raised when their raising event severity is changed maintain their original severity.

Facility Alarm Hierarchy

Facility Alarms for *children* objects is not raised for failure of a *parent* object. For example, when an fails (or is *shutdown*) there is not a set of port alarms raised.

When a parent alarm is cleared, children alarms that are still in occurrence on the node appears in the active alarms list. For example, when a port fails there is a port alarm, but if the port is later shutdown the port alarm is cleared (and a card alarm will be active for the). If the card comes back into service, and the port is still down, then a port alarm becomes active once again.

The supported Facility Alarm hierarchy is as follows (parent objects that are *down* cause alarms in all children to be masked):

- CPM -> Compact Flash
- IOM/IMM -> MDA -> Port -> Channel

Note that a *masked* alarm is not the same as a *cleared* alarm. The cleared alarm queue does not display entries for previously raised alarms that are currently masked. If the masking event goes away, then the previously raised alarms will once again be visible in the active alarm queue.

Facility Alarm List

The following table(s) show the supported Facility Alarms.

Table 43: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event

Alarm *1	Alarm Name/ Raising Event	Sample Details String	Clearing Event	7210 SAS Devices					
				M	X	T	Mxp	Sx	R6 and R12
7-2001-1	tmnxEqCardFailure	Class MDA Module: failed, reason: MDA 1 failed startup tests	tmnxChassisNotificationClear	N	N	N	N	N	Y
7-2003-1	tmnxEqCardRemoved	Class CPM Module: removed	tmnxEqCardInserted	N	N	N	N	N	Y
7-2004-1	tmnxEqWrongCard	Class IOM Module: wrong type inserted	tmnxChassisNotificationClear	N	N	N	N	N	Y
7-2005-1	tmnxEnvTempTooHigh	Chassis 1: temperature too high	tmnxChassisNotificationClear	Y	Y	Y	Y	Y	Y
7-2006-1	tmnxEqFanFailure	Fan 1 failed	tmnxChassisNotificationClear	Y	Y	Y	Y	Y	Y
7-2007-1	tmnxEqPowerSupplyFailureOvt	Power supply 2 over temperature	tmnxChassisNotificationClear	N	N	N	N	N	N
7-2008-1	tmnxEqPowerSupplyFailureAc	Power supply 1 AC failure	tmnxChassisNotificationClear	N	N	N	N	N	N

Table 43: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event

Alarm *1	Alarm Name/ Raising Event	Sample Details String	Clearing Event	7210 SAS Devices					
				M	X	T	Mxp	Sx	R6 and R12
7-2009-1	tmnxEqPowerSupplyFailureDc	Power supply 2 DC failure	tmnxChassisNotificationClear	N	N	N	N	N	N
7-2011-1	tmnxEqPowerSupplyRemoved	Power supply 1, power lost	tmnxEqPowerSupplyInserted	Y(ETR and Non-ETR)	Y	Y (ETR and Non-ETR)	Y (ETR and Non-ETR)	Y (ETR and Non-ETR)	Y
7-2017-1	tmnxEqSyncIfTimingHoldover	Synchronous Timing interface in holdover state	tmnxEqSyncIfTimingHoldoverClear	Y	Y	Y	Y	Y	Y
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Synchronous Timing interface, alarm loss on reference 1	tmnxEqSyncIfTimingRef1AlarmClear	Y	Y	Y	Y	Y	Y
7-2019-2	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oof(2)'	Synchronous Timing interface, alarm of on reference 1	same as 7-2019-1	Y	Y	Y	Y	Y	Y

Table 43: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event	7210 SAS Devices					
				M	X	T	Mxp	Sx	R6 and R12
7-2019-3	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	Synchronous Timing interface, alarm oopir on reference 1	same as 7-2019-1	Y	Y	Y	Y	Y	Y
7-2021-x	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2	Y	Y	Y	Y	Y	Y
7-2030-x	same as 7-2019-x but for the BITS1 input	same as 7-2019-x but for the BITS1 input	same as 7-2019-x but for the BITS1 input	N	N	Y	Y	N	Y
7-2033-1	tmnxChassisUpgradeInProgress	Class CPM Module: software upgrade in progress	tmnxChassisUpgradeComplete	N	N	N	N	N	N
7-2050-1	tmnxEqPowerSupplyFailureInput	Power supply 1 input failure	tmnxChassisNotificationClear	Y	Y	Y	Y	Y	Y

Table 43: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event	7210 SAS Devices					
				M	X	T	Mxp	Sx	R6 and R12
7-2051-1	tmnxEqPowerSupplyFailureOutput	Power supply 1 output failure	tmnxChassisNotificationClear	Y	Y	Y	Y	Y	Y
7-2073-x	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input	N	N	Y	Y	N	N
3-2004-1	linkDown	Interface intf-towards-node-B22 is not operational	linkUp	Y	Y	Y	Y	Y	Y

The linkDown Facility Alarm is supported for the following objects (note that all objects may not be supported on all platforms):

Table 44: linkDown Facility Alarm Support

Object	Supported?
Ethernet Ports	Yes
TDM Ports (E1, T1) including CES MDAs (only on 7210 SAS-M)	Yes
Ethernet LAGs	No
Ethernet VLANs	No

Configuring Logging with CLI

This section provides information to configure logging using the command line interface.

Topics in this section include:

- [Basic Facility Alarm Configuration on page 388](#)
- [Common Configuration Tasks on page 389](#)

Basic Facility Alarm Configuration

The most facility alarm configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays an alarm configuration example.

```
*7210SAS>config>system>alarms# info detail
-----
                no shutdown
                exit
-----
*7210SAS>config>system>alarms#
```

Common Configuration Tasks

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

- [Configuring the Maximum Number of Alarms To Clear on page 389](#)
-

Configuring the Maximum Number of Alarms To Clear

The number of alarms to clear can be configured using the command listed below.

Use the following CLI syntax to configure a log file:

CLI Syntax: `config>system
 alarms
 max-cleared max-alarms`

The following displays facility alarm configuration example:

```
ALA-12>config>system# alarms
-----
...
max-cleared 500
exit
...
-----
```

Facility Alarms Command Reference

Command Hierarchies

- [Facility Alarm Configuration Commands on page 391](#)
- [Show Commands on page 391](#)

Facility Alarm Configuration Commands

```
config
  — system
    — alarms
      — max-cleared max-alarms
      — [no] shutdown
```

Show Commands

```
show
  — system
    — alarms [cleared] [severity severity-level] [count count] [newer-than days]
```

Configuration Commands

Generic Commands

alarms

Syntax	alarms
Context	config>system
Description	This command enters the context to configure facility alarm parameters.

max-cleared

Syntax	max-cleared <i>max-alarms</i>
Context	config>system>alarms
Description	This command configures the maximum number of cleared alarms that the system will store and display.
Default	500
Parameters	<i>max-alarms</i> — Specify the maximum number of cleared alarms. Value: [0..500]

shutdown

Syntax	[no] shutdown
Context	config>system>alarms
Description	This command enables or disables the Facility Alarm functionality. When enabled, the Facility Alarm sub-system tracks active and cleared facility alarms and controls the Alarm LEDs on the CPMs/CFMs. When Facility Alarm functionality is enabled, the alarms are viewed using the <code>show system alarms</code> command(s). Note: Shutting down the system alarms clears all the existing alarms (raised and cleared). The user performing no shutdown will not bring back the earlier raised alarm.
Default	no shutdown

Show Commands

alarms

- Syntax** **alarms** [**cleared**] [**severity severity-level**] [**count count**] [**newer-than days**]
- Context** show>system
- Description** This command displays facility alarms on the system.
- Output** **Facility Alarm Output** — The following table describes the alarms output fields.

Sample Output

Table 45: Show Facility Alarms Output Fields

Label	Description
Index	Alarm index number.
Date/Time	Date and time string for the alarm.
Severity	Severity level of the alarm.
Alarm	Alarm identifier.
Resource	Facility associated with the alarm.
Details	Description of the alarm.

```
*A:7210SAS# show system alarms

=====
Alarms [Critical:1 Major:2 Minor:0 Warning:0 Total:3]
=====
Index      Date/Time          Severity    Alarm        Resource
  Details
-----
13 2014/11/13 14:34:39.20 MAJOR 7-2005-1 Chassis 1
    Chassis: Temperature too high

12 2014/11/13 14:34:13.70 MAJOR 7-3002-1 Alarm Input Module 2
    Alarm Input "Pin 2" ("2") has changed status to "alarm"
    "Alarm Input
    Triggered"

11 2014/11/13 14:32:37.00 CRITICAL 7-3001-1 Alarm Input Module 1
    Alarm Input "Pin 1" ("1") has changed status to "alarm"
    "Alarm Input
    Triggered"
=====
*A:7210SAS#
```

Show Commands

Cleared alarms table:

A:Dut-A# show system alarms cleared

```
=====
Cleared Alarms [Size:500 Total:5 (not wrapped)]
=====
Index      Date/Time          Severity    Alarm        Resource
  Details
-----
5          2011/04/01 18:11:55.00 MAJOR      7-2005-1     Chassis 1
  Clear Chassis temperature too high alarm

3          2011/04/01 18:11:54.50 CRITICAL   7-2051-1     Power Supply 1
  Clear Power Supply failure

2          2011/04/01 18:11:54.40 CRITICAL   7-2050-1     Power Supply 1
  Clear Power Supply failure

4          2011/04/01 18:11:54.10 MINOR      7-2004-1     Fan 1
  Clear Fan wrong type failure

1          2011/04/01 18:11:54.00 CRITICAL   7-2007-1     Power Supply 1
  Clear Power Supply failure
=====
```

Standards and Protocol Support



NOTE: The capabilities available when operating in access-uplink mode/L2 mode and network mode/MPLS mode are different. Correspondingly, not all the standards and protocols listed below are applicable to access-uplink mode and network mode.

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 802.1ah Provider Backbone Bridges (**Not Supported on 7210 SAS-Sx, 7210 SAS-R6 and 7210 SAS-Mxp**)
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ae 10Gbps Ethernet
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
draft-ietf-disman-alarm-mib-04.txt
IANA-IFTtype-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

BGP

RFC 1397 BGP Default Route Advertisement
RFC 1772 Application of BGP in the Internet
RFC 1997 BGP Communities Attribute

RFC 2385 Protection of BGP Sessions via MD5
RFC 2439 BGP Route Flap Dampening
RFC 2547bis BGP/MPLS VPNs draft-ietf-idr-rtc2858bis-09.txt.
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 3392 Capabilities Advertisement with BGP-4
RFC 4271 BGP-4 (previously RFC 1771)
RFC 4360 BGP Extended Communities Attribute
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)
RFC 4760 Multi-protocol Extensions for BGP
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 5291 Outbound Route Filtering
RFC 5668 4-Octet AS Specific BGP Extended Community Capability for BGP-4
draft-ietf-idr-add-paths, 04, Advertisement of Multiple Paths in BGP

CIRCUIT EMULATION (7210 SAS-M Only)

RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
RFC 5287 Control Protocol Extensions for the Setup of Time-Division

Multiplexing (TDM) Pseudowires in MPLS Networks

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
RFC 2697 A Single Rate Three Color Marker
RFC 2698 A Two Rate Three Color Marker
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic

IP Fast Reroute

NOTE: On 7210 only LDP FRR is supported.

RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates
IPv6 (Not supported on 7210 SAS-Sx)
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

Standards and Protocols

RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing
RFC 2740 OSPF for IPv6
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 4552 Authentication/Confidentiality for OSPFv3
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
draft-ietf-isis-ipv6-05
draft-ietf-isis-wg-multi-topology-xx.txt

IS-IS

RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
RFC 2763 Dynamic Hostname Exchange for IS-IS
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
RFC 3567 Intermediate System to Intermediate System (ISIS) Cryptographic Authentication
RFC 3719 Recommendations for Interoperable Networks using IS-IS
RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC 3787 Recommendations for Interoperable IP Networks
RFC 3847 Restart Signaling for IS-IS – GR helper
RFC 4205 for Shared Risk Link Group (SRLG) TLV

MPLS - General

RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

MPLS - LDP

RFC 5036 LDP Specification
RFC 3037 LDP Applicability
RFC 3478 Graceful Restart Mechanism for LDP — GR helper
RFC 5283 LDP extension for Inter-Area LSP
RFC 5443 LDP IGP Synchronization
RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to- Multipoint Label Switched Paths (Applicable only for 7210 SAS-T, 7210 SAS-Mxp, 7210 SAS-R6, and 7210 SAS-R12)

MPLS - RSVP-TE

RFC 2430 A Provider Architecture DiffServ & TE
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC2747 RSVP Cryptographic Authentication
RFC3097 RSVP Cryptographic Authentication
RFC 3209 Extensions to RSVP for Tunnels
RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels
RFC 5817 Graceful Shutdown in MPLS and GMPLS Traffic Engineering Networks
RFC 2961 RSVP Refresh Overhead Reduction Extensions

MPLS-TP (Transport Profile) [7210 SAS-T in network mode only, 7210 SAS-R6 and 7210 SAS-R12]

RFC 5586 MPLS Generic Associated Channel
RFC 5921 A Framework for MPLS in Transport Networks

RFC 5960 MPLS Transport Profile Data Plane Architecture
RFC 6370 MPLS-TP Identifiers
RFC 6378 MPLS-TP Linear Protection
RFC 6428 Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile
RFC 6426 MPLS On-Demand Connectivity and Route Tracing
RFC 6478 Pseudowire Status for Static Pseudowires
draft-ietf-mpls-tp-ethernet-addressing-02 MPLS-TP Next-Hop Ethernet Addressing

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) [Only in 7210 SAS-M and 7210 SAS-T access-uplink mode and supported with IPv4 Multicast in network mode]
RFC 2362 Protocol Independent Multicast Sparse Mode (PIM-SM)
RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast (MLDv2 is not supported)
RFC 4607 Source-Specific Multicast for IP
RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
draft-ietf-pim-sm-bsr-06.txt

Multicast VPNs (Multicast VPN support is only supported on 7210 SAS-T, 7210 SAS-Mxp, 7210 SAS-R6 and 7210 SAS-R12)

RFC 6512, Using Multipoint LDP When the Backbone Has No Route to the Root
RFC 6513, Multicast in MPLS/BGP IP VPNs

Standards and Protocols

RFC 6514, BGP Encodings and Procedures for Multicast in MPLS/IP VPNs
RFC 6515, IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs (Only IPv4 family is supported)
RFC 7385, IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points

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 2206 RSVP-MIB
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASEDSMMIB
RFC 2575 SNMP-VIEW-BASEDACM-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-MI
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-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt

OSPF

RFC 1765 OSPF Database Overflow
RFC 2328 OSPF Version 2
RFC 2370 Opaque LSA Support
RFC 3101 OSPF NSSA Option
RFC 3137 OSPF Stub Router Advertisement
RFC 3623 Graceful OSPF Restart – GR helper
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospf-ospfv3-update-14.txt
RFC 4203 Shared Risk Link Group (SRLG) sub-TLV
RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)

PSEUDO-WIRE

RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
RFC 4446 IANA Allocations for PWE3

RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge
draft-ietf-l2vpn-vpws-iw-oam-02.txt, OAM Procedures for VPWS Interworking
RFC6310, Pseudowire (PW) OAM Message Mapping
RFC6073, Segmented Pseudowire (draft-ietf-pwe3-segmented-pw-18.txt)
draft-ietf-pwe3-dynamic-ms-pw-14.txt, Dynamic Placement of Multi Segment Pseudo Wires
draft-ietf-pwe3-redundancy-bit-06.txt, Pseudowire Preferential Forwarding Status bit definition
draft-ietf-pwe3-redundancy-06.txt, Pseudowire (PW) Redundancy
RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network (Applicable to only 7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12);

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

Standards and Protocols

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
draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base
RFC 5880 Bidirectional Forwarding Detection
RFC 5881 BFD IPv4 (Single Hop)
RFC 5883 BFD for Multihop Paths

Timing (Not applicable for 7210 SAS-Sx)

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. (Not applicable for 7210 SAS-Sx)
IEEE Std 1588™-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. (Not applicable for 7210 SAS-Sx)

VPLS

RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)

VRRP

RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-M-V8v0.mib (7210 SAS-M Only)
TIMETRA-CAPABILITY-7210-SAS-X-V8v0.mib (7210 SAS-X Only)
TIMETRA-CAPABILITY-7210-SAS-R-V8v0.mib (only 7210 SAS-R6 and 7210 SAS-R12)
TIMETRA-CAPABILITY-7210-SAS-T-V8v0.mib (only 7210 SAS-T)
TIMETRA-CAPABILITY-7210-SAS-Mxp-V8v0.mib (7210 SAS-Mxp Only)
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
TIMETRA-SAS-FILTER-MIB.mib

TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-IEEE8021-PAE-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-LOG-MIB.mib.mib
TIMETRA-SAS-MIRROR-MIB.mib
TIMETRA-SAS-MPOINT-MGMT-MIB.mib (Only for 7210 SAS-X)
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SDP-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SAS-SERV-MIB.mib
TIMETRA-SAS-VRTR-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-ISIS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-VRRP-MIB.mib
TIMETRA-VRTR-MIB.mib

INDEX

B

BOF

- overview
 - compact flash
 - storing log files 215

L

Log

- overview 212, 378
 - accounting 230
 - accounting records 230
 - default system log 229
 - destinations 214
 - event control 222
 - event filter policies 225
 - event log entries 226
 - event logs 219
 - event sources 220
 - log files 215
 - log manager 224
 - SNMP trap groups 217
 - syslog 217
- configuring
 - accounting policy 277
 - basic 273, 388
 - command reference
 - file ID commands 302
 - filter commands 302
 - log ID commands 304
 - syslog commands 305
 - event control 278
 - event log 274, 389
 - file ID 276
 - log filter 280
 - log types 272
 - management tasks 283
 - overview 272
 - SNMP trap group 281
 - syslog target 282

S

Security

- overview
 - AAA 18
 - accounting 26
 - RADIUS 26
 - TACACS+ 26
 - authentication 19
 - RADIUS 20
 - TACACS+ 23
 - authorization 24
 - 24
 - local 25
 - RADIUS 25
 - TACACS+ 25
 - controls 28
 - encryption 41
 - SSH 37
 - configuring
 - accounting 51
 - RADIUS 66
 - TACACS+ 70
 - authentication 48
 - RADIUS 64
 - TACACS+ 67
 - authorization 49
 - RADIUS 65
 - TACACS+ 69
 - basic 52
 - login controls 72
 - management access filters 55
 - password management 56
 - profiles 57
 - SSH 71
 - users 58
 - encryption 41
 - keychains 44
 - SSH 37
 - VSAs 30
 - Alcatel-Lucent Dictionary 34

SNMP

- overview
 - access control 164
 - access groups 165

Index

- users 166
- USMs 165
- views 165
- architecture 162
- MIBs 162
- versions 163
- configuring
 - access options 177
 - basic 173
 - command reference
 - security commands 181
 - show commands 182, 391
 - system commands 181
 - community strings 175
 - SNMPv1 and SNMPv2 172
 - SNMPv3 172
 - USM community options 179
 - view options 176
 - command reference
 - system commands 181
 - user commands 182