NOKIA

7210 SERVICE ACCESS SWITCH

7210 SAS OS System Management Guide
7210 SAS-D,
7210 SAS-E,
7210 SAS-K2F2T1C
7210 SAS-K2F4T6C
Release 9.0.R4

3HE11488AAADTQZZA

Issue: 1

April 2017

TABLE OF CONTENTS

SNMP

NETCONF

Event and Accounting Logs

Facility Alarms

List of Tables

Getting Started

Security

SNMP

NETCONF

Event and Accounting Logs

Facility Alarms

LIST OF FIGURES

Security

SNMP

NETCONF

Event and Accounting Logs

Facility Alarms

Preface

About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure 7210 SAS-D, E, K platforms 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 not supported on a particular platform.

NOTES:

- 7210 SAS-K5 stands for 7210 SAS-K 2F2T1C and 7210 SAS-K12 stands for 7210 SAS-K 2F4T6C platforms.
- 7210 SAS-E, 7210 SAS-D, and 7210 SAS-K 2F2T1C operate in access-uplink mode by default. No explicit user configuration is needed for this. 7210 SAS-K 2F4T6C operates in both Access-uplink and Network Mode.

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 D, E, K 2F2T1C and K 2F4T6C OS documentation set is composed of the following books:

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), link aggregation group (LAG) and port provisioning.

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C 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-K 2F2T1C and 7210 SAS-K 2F4T6C OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for OSPF, IS-IS and route policies. 7210-SAS D, E, K 2F2T1C and K 2F4T6C OSServices Guide

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C 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-K 2F4T6C OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).

- 7210-SAS D, E, K 2F2T1C and K 2F4T6C OS Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.

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.

Nokia 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 19
Network management	Configure SNMP elements.	SNMP on page 159
Operational functions	Configure event and accounting logs.	Event and Accounting Logs on page 271
Reference	List of IEEE, IETF, and other proprietary entities.	

Security

In This Chapter

The following topics in this chapter provide information to configure security parameters:

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.

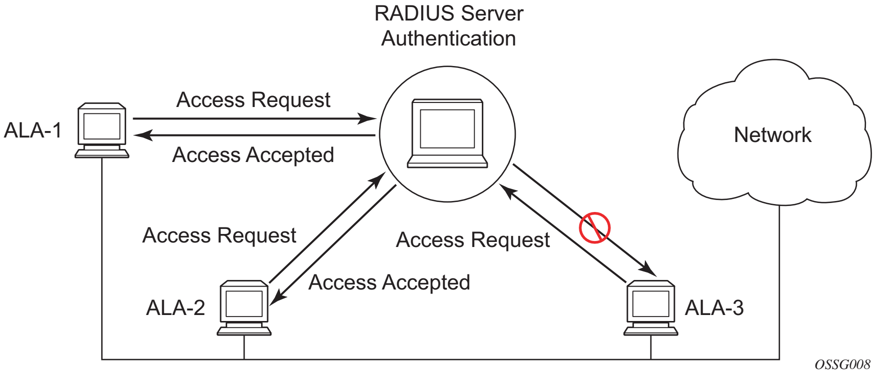


Figure 1: RADIUS Requests and Responses

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 22
- RADIUS Authentication on page 22
- TACACS+ Authentication on page 25

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 is 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 23).

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 log on 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 31.

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 26
- RADIUS Authorization on page 26
- TACACS+ Authorization on page 27

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 time-stamp.

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 Nokia’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.

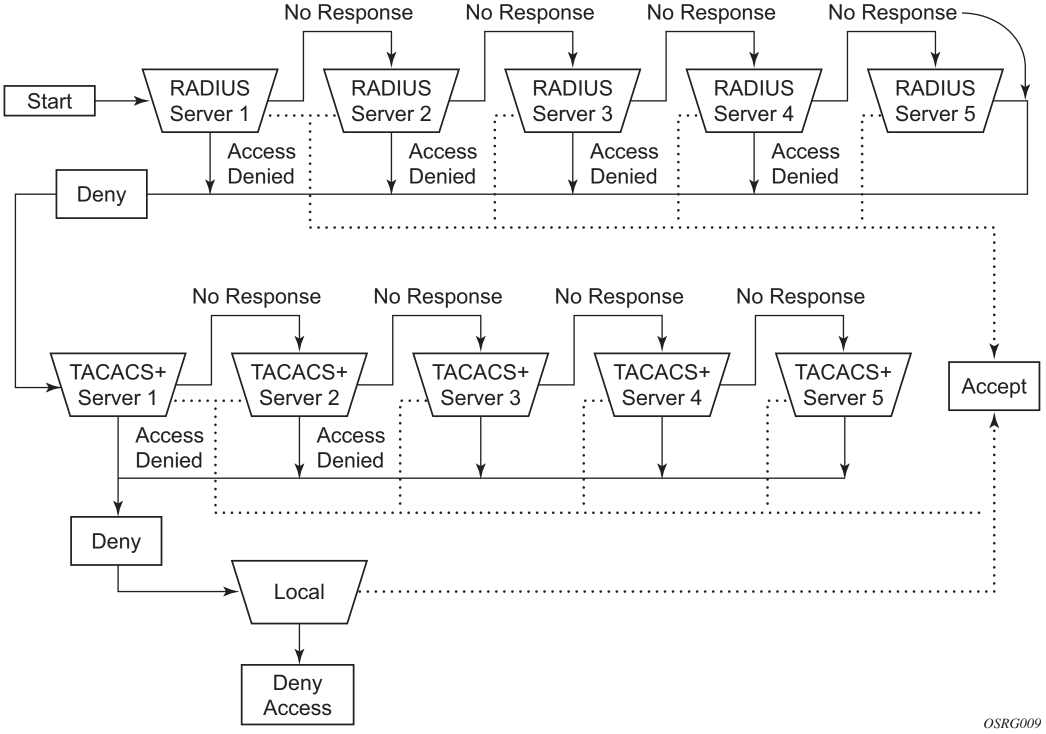


Figure 2: Security Flow

Vendor-Specific Attributes (VSAS)

The OS supports the configuration of Nokia-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 Nokia-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 Nokia.

- `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.

The software supports the configuration of Nokia-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 Nokia-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 Nokia.

- 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.

  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.

  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,
```

Nokia Dictionary

```
# Revision: 1.29.6.2

VENDOR          Nokia-IPD               6527

# User management VSAS
ATTRIBUTE Timetra-Access                    1      integer Nokia-IPD

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

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

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

ATTRIBUTE Timetra-Profile                   4      string  Nokia-IPD
ATTRIBUTE Timetra-Default-Action            5      integer Nokia-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  Nokia-IPD
ATTRIBUTE Timetra-Action                    7      integer Nokia-IPD

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

ATTRIBUTE Timetra-Exec-File                 8      string  Nokia-IPD

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

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

ATTRIBUTE Alc-Client-Hardware-Addr         27      string  Nokia-IPD
ATTRIBUTE Alc-Int-Dest-Id-Str              28      string  Nokia-IPD
ATTRIBUTE Alc-Primary-Nbns                 29      ipaddr  Nokia-IPD
ATTRIBUTE Alc-Secondary-Nbns               30      ipaddr  Nokia-IPD
ATTRIBUTE Alc-MSAP-Serv-Id                 31      integer Nokia-IPD
ATTRIBUTE Alc-MSAP-Policy                  32      string  Nokia-IPD
ATTRIBUTE Alc-MSAP-Interface               33      string  Nokia-IPD
ATTRIBUTE Alc-PPPoE-PADO-Delay             34      integer Nokia-IPD
ATTRIBUTE Alc-PPPoE-Service-Name           35      string  Nokia-IPD
ATTRIBUTE Alc-DHCP-Vendor-Class-Id         36      string  Nokia-IPD

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

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

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

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

# Match TC TmnxAuthAlgorithm in TIMETRA-IPSEC-MIB
VALUE     Alc-IPsec-SA-Auth-Algorithm     null            1
VALUE     Alc-IPsec-SA-Auth-Algorithm     md5             2
VALUE     Alc-IPsec-SA-Auth-Algorithm     sha1           3

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

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

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

#credit control VSAS
ATTRIBUTE Alc-Credit-Control-CategoryMap   95      string  Nokia-IPD
ATTRIBUTE Alc-Credit-Control-Quota         96      string  Nokia-IPD

ATTRIBUTE Alc-Force-Nak                    98      string  Nokia-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 places 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.

NOTE: 7210 SAS-D and 7210 SAS-E supports SSH for both IPv4 and IPv6. 7210 SAS-K 2F2T1C and SAS-K 2F4T6C supports SSH for only IPv4.

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 “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 Back-off

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 86.

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 Nokia 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

```
0                  1                 2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Kind     | Length      |T|K|   Alg ID|Res|         Key ID |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Authentication Data |
                      | // |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 and 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*. They 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 *algorithm* parameter. config>system>security>keychain>direction>uni>receive>entry with algorithm *algorithm* parameter. config>system>security>keychain>direction>uni>send>entry with algorithm *algorithm* 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).

Table 4: Keychain Mapping (Continued)

Field	Definition	CLI
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 31.

- 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 31.

  → 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

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 317
- 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

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 one keyword 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

          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
orithm aes-128-cmac-96
                            begin-time 2006/12/18 22:55:20
                        exit
                    exit
                exit
            exit
            keychain "baSASd"
                direction
                    uni
                        receive
                            entry 1 key "Ee7xdKlYO2DOm7v3IJv/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

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 31.

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 D, E, K 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.

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 79
  - → Keychain Commands on page 79
  - → TCP Enhanced Authentication Commands on page 79
- Login Control Commands on page 80
- Show Commands on page 80
- 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
            — [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 criteria for management access filters is not supported on 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C.

```
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
                    — complexity-rules
                         — [no] allow-user-name
                         — credits [lowercase credits] [uppercase credits] [numeric credits]
                           [special-character credits]
                         — no credits
                         — minimum-classes minimum
                         — no minimum-classes
                         — minimum-length length
                         — no minimum-length
                         — repeated-characters count
                         — no repeated-characters
                         — required [lowercase count] [uppercase count] [numeric count]
                           [special-character count]
                         — no required
                    — [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| for-
                          ever}
                        — 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| for-
                          ever}
                        — [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
```

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]
```

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** *description-string*
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 *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

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 This command creates the context to configure security settings.

Security commands manage user profiles and user membership. Security commands also manage user login registrations.

ftp-server

Syntax [**no**] **ftp-server**

Context config>system>security

Description This command enables FTP servers running on the system.

FTP servers are disabled by default. At system startup, only SSH server are enabled.

The **no** form of the command disables FTP servers running on the system.

hash-control

Syntax **hash-control** [**read-version** {**1** | **2** | **all**}] [**write-version** {**1** | **2**}]
no hash-control

Context config>system>security

Description 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.

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.

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.

Default all — read-version set to accept both versions 1 and 2

Parameters **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.

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.

source-address

Syntax **source-address**

Context config>system>security

Description This command specifies the source address that should be used in all unsolicited packets sent by the application.

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.

application

Syntax **application** *app* [*ip-int-name*|*ip-address*]
no application *app*

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 *app* — Specify the application name.

Values telnet, ftp, ssh, radius, tacplus, snmptrap, syslog, ping, traceroute, dns, sntp, ntp
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.

ip-int-name | *ip-address* — 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.

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 *minutes* — 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** *value*
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 *value* — The maximum number of concurrent FTP sessions on the node.

Values 0 — 5

inbound-max-sessions

Syntax **inbound-max-sessions** *value*
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 *value* — 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** {**url** *url-prefix*: *source-url* | **text** *motd-text-string*}
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** *url-prefix*: *source-url* — 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 *motd-text-string* **—** The text of the message of the day. The *motd-text-string* 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** *value*
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 *value* — The maximum number of concurrent outbound Telnet sessions, expressed as an integer.

Values 0 — 7

pre-login-message

Syntax **pre-login-message** *login-text-string* [**name**]
no pre-login-message

Context config>system>login-control

Description 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.

It is possible to add the name parameter to an existing message without affecting the current **pre-login-message**.

The **no** form of the command removes the message.

Default No **pre-login-message** is defined.

Parameters *login-text-string* — 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.

name — When the keyword *name* 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.

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 This command enables graceful shutdown of SSH sessions.

The **no** form of the command disables graceful shutdown of SSH sessions.

preserve-key

Syntax [**no**] **preserve-key**

Context config>system>security>ssh

Description 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.

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.

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 *ssh-version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1
2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2
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.

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 [**no**] **management-access-filter**

Context config>system>security

Description This command creates the context to edit management access filters and to reset match criteria.

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.

Management filters, as opposed to other traffic filters, are enforced by system software.

The **no** form of the command removes management access filters from the configuration.

Default No management access filters are defined.

ip-filter

Syntax [**no**] **ip-filter**

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

Description This command enables the context to configure management access IP filter parameters.

ipv6-filter

Syntax [**no**] **ipv6-filter**

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

Description **Platforms Supported:** 7210 SAS-D and 7210 SAS-E.

NOTE: On 7210 SAS-K IPv6 criteria for Management Access Filters is not supported.

This command enables the context to configure management access IPv6 filter parameters.

default-action

Syntax **default-action** {**permit | deny | deny-host-unreachable**}

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K2F2T1C and 7210 SAS-K2F4T6C supports only IPv4 filters.

This command creates the default action for management access in the absence of a specific management access filter match.

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.

Default No default-action is defined.

Parameters **permit —** Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.

deny — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued..

deny-host-unreachable — Specifies that packets not matching the selection criteria be denied and a host unreachable message will be issued.

entry

Syntax [**no**] **entry** *entry-id*

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K2F2T1C and 7210 SAS-K2F4T6C supports only IPv4 filters.

This command is used to create or edit a management access filter entry. Multiple entries can be created with unique *entry-id* 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.

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.

The **no** form of the command removes the specified entry from the management access filter.

Default No entries are defined.

Parameters *entry-id* — 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.

Values 1 — 9999

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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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`

Format Style	Format Syntax	Example
Hexadecimal	`0xHHHH`	`0xF800`
Binary	`0bBBBBBBBBBBBBBBBB`	`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 **Platforms Supported:** 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion.

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.

The no form of the command removes the match criterion.

Default no fragment

Parameters *true* — 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.

false — 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.

l4-src-port

Syntax **[no] l4-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 **Platforms Supported:** 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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.

The no form of the command removes the source port match criterion.

Default no l4-src-port

Parameters *port* — The source port number to be used as a match criteria expressed as a decimal integer.

Values [1..65535]

mask — Specifies the mask in dotted decimal notation

Values [1..65535]decimal hex or binary

flow-label

Syntax **flow-label** *value*
no flow-label

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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 non default 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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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*

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

This command configures an IP protocol type to be used as a management access filter match criterion.

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).

The **no** form the command removes the protocol from the match criteria.

Default No protocol match criterion is specified.

Parameters *protocol* — The protocol number for the match criterion.

Values 1 - 255 (decimal)

router

Syntax **router** {*router-instance*}
no router

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 77210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

The command configures a router name or service ID to be used as a management access filter match criterion.

The **no** form of the command removes the router name or service ID from the match criteria.

Default Base

Parameters *router-instance* — Specifies the router name.

Default Base

Values Base, Vpls-management (for 7210 SAS D)

Values Base, Management, Vpls-management (for 7210 SAS E)

renum

Syntax **renum** *old-entry-number new-entry-number*

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

This command renumbers existing management access filter entries to re-sequence filter entries.

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.

Parameters *old-entry-number* — 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

src-port

Syntax **src-port** {*port-id* **|** **lag** *lag-id*}
no src-port

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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

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 *port-id* — 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

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 filters. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 filters.

This command configures a source IP address range to be used as a management access filter match criterion.
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.

The **no** form of the command removes the source IP address match criterion.

Default No source IP match criterion is specified.

Parameters *ip-prefix/prefix-length* — The IP prefix used for IP match criteria in dotted decimal notation. Can be IPv4 or an IPv6 prefix.

ipv4-prefix: a.b.c.d

```
ipv4-prefix-length: 0 — 32
ipv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)
                   x:x:x:x:x:x:d.d.d.d
                         x: [0..FFFF]H
                         d: [0..255]D
ipv6-prefix-length: 0 — 128
```

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

Password Commands

admin-password

Syntax **admin-password** *password* [**hash** | **hash2**]
no admin-password

Context config>system>security>password

Description This command allows a user (with admin permissions) to configure a password which enables a user to become an administrator.

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.

This functionality can be enabled in two contexts:

config>system>security>password>admin-password

<global> enable-admin

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.

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

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

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

NOTE: The *password* argument of this command is not sent to the servers. This is consistent with other commands which configure secrets.

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.

For example:

```
file copy ftp://test:secret@131.12.31.79/test/srcfile cf1:\destfile
```

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 '****'.

The **no** form of the command removes the admin password from the configuration.

Default no admin-password

Parameters *password* — 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.

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

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 **NOTE:** See the description for the **admin-password** on the previous page. If the **admin-password** is configured in the config>system>security>password context, then any user can enter the special administrative mode by entering the **enable-admin** command.

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

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

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

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

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

```
A:ALA-1# show users
===============================================================================
User Type From Login time Idle time
===============================================================================
admin Console -- 10AUG2006 13:55:24 0d 19:42:22
admin Telnet 10.20.30.93 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** *days*
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 *days* — The maximum number of days the password is valid.

Values 1 — 500

attempts

Syntax **attempts** *count* [**time** *minutes1* [**lockout** *minutes2*]
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 *minutes*: **5**
lockout *minutes*: **10**

Parameters *count* — 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** [*method-1*] [*method-2*] [*method-3*] [**exit-on-reject**]
no authentication-order

Context config>system>security>password

Description This command configures the sequence in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.

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.

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.

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

Default **authentication-order radius tacplus local** - The preferred order for password authentication is 1. RADIUS, 2. TACACS+ and 3. local passwords.

Parameters *method-1* — The first password authentication method to attempt.

Default **radius**

Values radius, tacplus, local

method-2 — The second password authentication method to attempt.

Default **tacplus**

Values radius, tacplus, local

method-3 — The third password authentication method to attempt.

Default **local**

Values radius, tacplus, local

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-rules

Syntax **complexity**-rules

Context config>system>security>password

Description This defines a list of rules for configurable password options.

allow-user-name

Syntax [**no**] **allow-user-name**

Context config>system>security>password>complexity-rules

Description The user name is allowed to be used as part of the password.

The **no** form of the command does not allow user name to be used as password

credits

Syntax **credits** [**lowercase** *credits*] [**uppercase** *credits*] [**numeric** *credits*] [**special-character** *credits*]
no credits

Context config>system>security>password>complexity-rules

Description The maximum credits given for usage of the different character classes in the local passwords.

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

Default no credits

Parameters *credits* — The number of credits that can be used for each characters class.

Values 0-10

minimum-classes

Syntax **minimum-classes** *minimum*
no minimum-classes

Context config>system>security>password>complexity-rules

Description Force the use of at least this many different character classes

The no form of the command resets to default.

Default no minimum-classes

Parameters *minmum* — The minimum number of classes to be configured.

Values 2-4

minimum-length

Syntax **minimum-length** *length*
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 *value* — The minimum number of characters required for a password.

Values 1 — 8

repeated-characters

Syntax **repeated-characters** *count*
no repeated-characters

Context config>system>security>password>complexity-rules

Description The number of times a characters can be repeated consecutively.

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

Default no repeated-characters

Parameters *count* — The minimum count of consecutively repeated characters.

Values 2-8

required

Syntax **required** [**lowercase** *count*] [**uppercase** *count*] [**numeric** *count*] [**special-character** *count*]
no required

Context config>system>security>password>complexity-rules

Description Force the minimum number of different character classes required.

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

Default no required

Parameters *count* — The minimum count of characters classes.

Values 0-10

complexity

Syntax [**no**] **complexity** [**numeric**] [**special-character**] [**mixed-case**]

Context config>system>security>password

Description This command configures the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and des-keys configured in the **authentication** section.

If more than one complexity command is entered, each command overwrites the previous command.

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.
For example, **no complexity numeric.**

Default No complexity requirements are configured.

Parameters **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.

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.

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. 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** *interval*]

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 *interval* — Specifies the interval of the health check in seconds.

Values 6 — 1500

minimum-length

Syntax **minimum-length** *value*
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 *value* — The minimum number of characters required for a password.

Values 1 — 8

password

Syntax **password**

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 *user-profile-name*>entry *entry-id*

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** *command-string*
no match

Context config>system>security>profile *user-profile-name*>entry *entry-id*

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 *command-string* — The CLI command or CLI tree level that is the scope of the profile entry.

copy

Syntax **copy** {**user** *source-user* | **profile** *source-profile*} **to** *destination* [**overwrite**]

Context config>system>security

Description This command copies a profile or user from a source profile to a destination profile.

Parameters *source-profile* — The profile to copy. The profile must exist.

dest-profile — The copied profile is copied to the destination profile.

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 *user-profile-name*

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** *description-string*
no description

Context config>system>security>profile *user-profile-name*>entry *entry-id*

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 *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

entry

Syntax [**no**] **entry** *entry-id*

Context config>system>security>profile *user-profile-name*

Description This command is used to create a user profile entry.

More than one entry can be created with unique *entry-id* 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.

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.

The **no** form of the command removes the specified entry from the user profile.

Default No entry IDs are defined.

Parameters *entry-id* — An entry-id uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the *entry-ids* should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.

Values 1 — 9999

profile

Syntax [**no**] **profile** *user-profile-name*

Context config>system>security

Description This command creates a context to create user profiles for CLI command tree permissions.

Profiles are used to either deny or permit user console access to a hierarchical branch or to specific commands.

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 *user-profile-name* can consist of up to 32 alphanumeric characters.

The **no** form of the command deletes a user profile.

Default user-profile default

Parameters *user-profile-name* — 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.

renum

Syntax **renum** *old-entry-number new-entry-number*

Context config>system>security>profile *user-profile-name*

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 [**no**] **access** [**ftp**] [**snmp**] [**console**]

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

Description This command grants a user permission for FTP, SNMP, console or lawful intercept (LI) access.

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.

The **no** form of command removes access for a specific application.
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.

Default No access is granted to the user by default.

Parameters **ftp —** Specifies FTP permission.

snmp — Specifies SNMP permission. This keyword is only configurable in the **config>system>security>user** context.

console — Specifies console access (serial port or Telnet) permission.

authentication

Syntax **authentication** {[**none**] **|** [[**hash**] {**md5** *key-1* **|** **sha** *key-1*} **privacy** {*privacy-level key-2*}]

Context config>system>security>user>snmp

Description 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.

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 *key* parameter.

Default **authentication none** - No authentication is configured and privacy cannot be configured.

Parameters **none —** Do not use authentication. If **none** is specified, then privacy cannot be configured.

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.

md5 *key* **—** The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.

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** *group-name*
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 *group-name* — 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** *source-user* **|** **profile** *source-profile*} **to** *destination* [**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 *source-user* — The user to copy. The user must already exist.

dest-user — 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** *url-prefix* [*directory*] [*directory***/***directory…*]

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 *local-url-prefix* [*directory*] [*directory/directory…*] — The user's local home directory URL prefix and directory structure up to 190 characters in length.

profile

Syntax **profile** *user-profile-name*
no profile

Context config>system>security>user-template

Description This command configures the profile for the user based on this template.

Parameters *user-profile-name* — 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** *url-prefix***:** *source-url*

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 *url-prefix: source-url* — 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** *user-profile-name* [*user-profile-name…up to 8max*]
no member *user-profile-name*

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 *user-profile-name* — 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** [*password*] [**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,

```
config>system>security# user testuser1
config>system>security>user$ password "zx/Uhcn6ReMOZ3BVrWcvk." hash2
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.

7210 SAS OS 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** *user-name*

Context admin

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

If a new *user-name* is entered, the user is created. When an existing *user-name* is specified, the user parameters can be edited.

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.

The **no** form of the command deletes the user and all configuration data. Users cannot delete themselves.

Default none

Parameters *user-name* — 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** *port*
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 *port* — 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** *port*
no port

Context config>system>security>radius

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, *Remote Authentication Dial In User Service* (*RADIUS*))

Parameters *port* — 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 7210 SAS seriesrouter.

Implement redundancy by configuring multiple server addresses for each 7210 SAS series 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 *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>radius

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 for management of the node. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 for management of the node.

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:x (eight 16-bit pieces) x: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** *seconds*
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 *seconds* — 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** *index* **address** *ip-address* **secret** *key*
no server *index*

Context config>system>security>tacplus

Description **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 for management of the node. 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C supports only IPv4 for management of the node.

This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.

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.

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

Default No TACACS+ servers are configured.

Parameters *index* — 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.

Values 1 — 5

address *ip-address* **—** 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.

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

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

Values Up to 128 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.

Values

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

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** *second*s
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** *name* [**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 *name* — Specifies the name of the RADIUS policy.

Values 1 — 32 characters

create — This keyword is mandatory to create a RADIUS policy.

retry

Syntax **retry** *count*
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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 for management of the node. 7210 SAS-K2F2T1C and 7210 SAS-K2F4T6C supports only IPv4 for management of the node.

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 Up to 128 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.

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

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

Values ip-address : a.b.c.d

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** *keychain-name*

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 *keychain-name* — 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.

Default There are no default entries.

Parameters *entry-id* — Specifies an entry that represents a key configuration to be applied to a keychain.

Values 0 — 63

key — Specifies a key ID which is used along with *keychain-name* and **direction** to uniquely identify this particular key entry.

authentication-key — Specifies the *authentication-key* that will be used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.

The *authentication-key* can be any combination of letters or numbers. .

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.

algorithm-*algorithm* — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.

Values aes-128-cmac-96 — Specifies an algorithm based on the AES standard
hmac-sha-1-96 — Specifies an algorithm based on SHA-1.

hash-key | *hash2-key* — The hash key. The key can be any combination of ASCII characters up to 33 for the *hash-key* and 96 characters for the *hash2-key* in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

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.

begin-time

Syntax **begin-time** [*date] [hours-minutes*] [**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 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.

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.

Parameters *date hours-minutes* — Specifies the date and time for the key to become active.

Values date: YYYY/MM/DD
hours-minutes: hh:mm[:ss]

now — Specifies the the key should become active immediately.

forever — Specifies that the key should always be active.

end-time

Syntax **end-time** [*date] [hours-minutes*] [**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 *date* — 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.

hours-minutes — 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.

UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.

now — Specifies a time equal to the current system time.

forever — Specifies a time beyond the current epoch.

tolerance

Syntax **tolerance** [*seconds* **| 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 *seconds* — Specifies the duration that an eligible receive key overlaps with the active send key.

Values 0 — 4294967294 seconds

forever — Specifies that an eligible receive key overlap with the active send key forever.

tcp-option-number

Syntax **tcp-option-number**

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** [*group-name*]

Context show>system>security

Description This command displays SNMP access group information.

Parameters *group-name* — 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
```

```
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. mgmt — The unique SNMP community string assigned to the management router.
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** [*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.

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 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-unreachble — 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 **Platforms Supported**: 7210 SAS-D, 7210 SAS-E

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-unreachble — 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 **Platforms supported**: 7210 SAS-D and 7210 SAS-E supports both IPv4 and IPv6 for management of the node. 7210 SAS-K2F2T1C and 7210 SAS-K2F4T6C supports only IPv4 for management of the node.

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.
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

```
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`	`Yes` — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device. `No` — The user is allowed to navigate to a directory higher in the directory tree on the home directory device.
`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                                                 included
read1             1.1.1.1                         11111111          included
write1            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#
```

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.

SNMP

In This Chapter

This chapter provides information to configure SNMP.

Topics in this chapter include:

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 Nokia (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 Nokia’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 as 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 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 provide 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.

Nokia'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 Nokia 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.

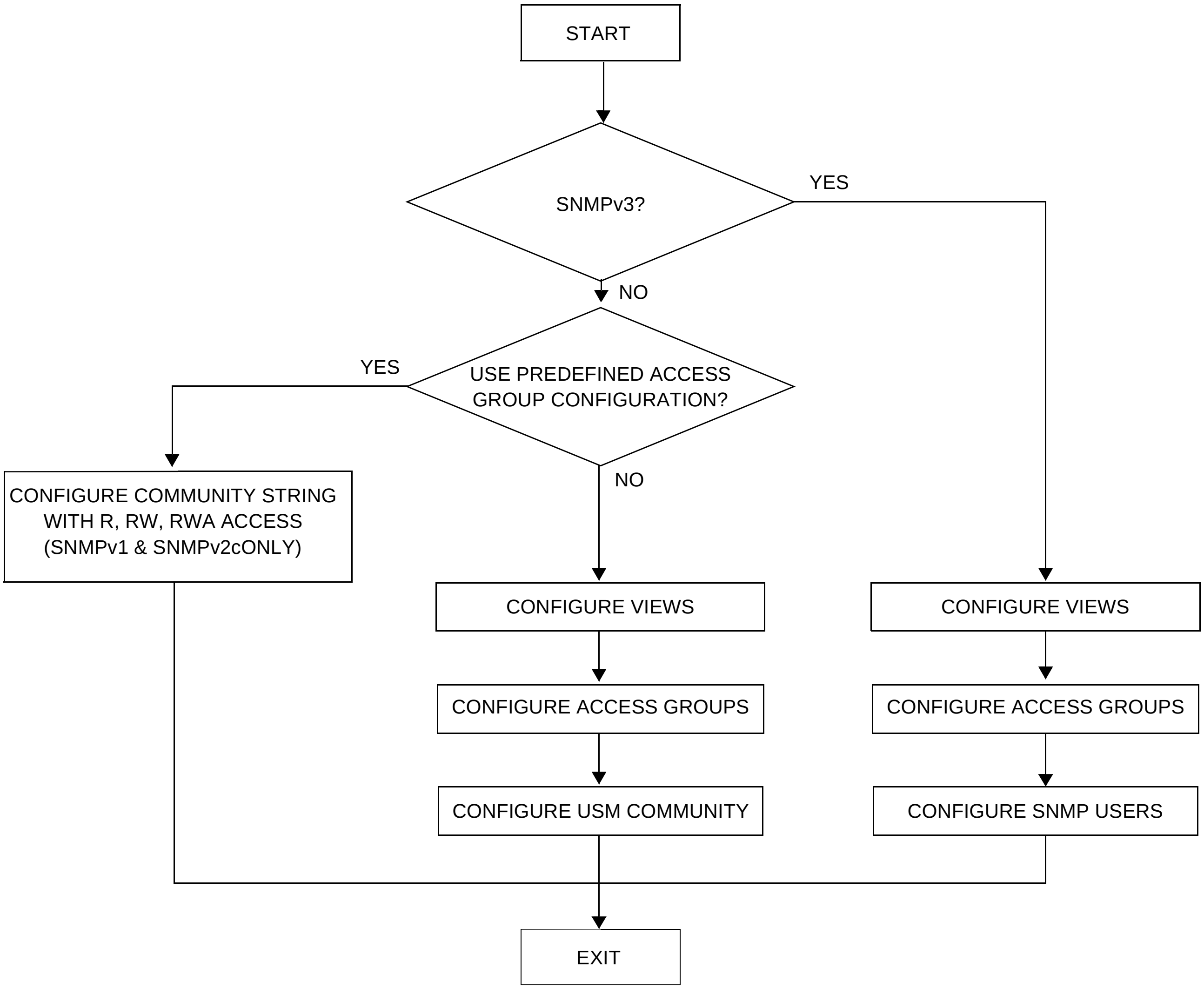


Figure 3: SNMPv1 and SNMPv2c Configuration and Implementation Flow

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 170
- Basic SNMP Security Configuration on page 171
- Configuring SNMP Components on page 172

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

Nokia 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-
vacy read no-security notify no-security
                access group snmp-ro security-model snmpv2c security-level no-auth-no-pri-
vacy read no-security notify no-security
                access group snmp-rw security-model snmpv1 security-level no-auth-no-pri-
vacy read no-security write no-security notify no-security
                access group snmp-rw security-model snmpv2c security-level no-auth-no-pri-
vacy read no-security write no-security notify no-security
                access group snmp-rwa security-model snmpv1 security-level no-auth-no-pri-
vacy read iso write iso notify iso
               access group snmp-rwa security-model snmpv2c security-level no-auth-no-pri-
vacy read iso write iso notify iso
               access group snmp-trap security-model snmpv1 security-level no-auth-no-pri-
vacy notify iso
                access group snmp-trap security-model snmpv2c security-level no-auth-no-
privacy notify iso
                attempts 20 time 5 lockout 10
```

Configuring SNMP Components

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

- Configuring a Community String on page 173
- Configuring View Options on page 174
- Configuring Access Options on page 175
- Configuring USM Community Options on page 177
- Configuring Other SNMP Parameters on page 178

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-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:cses-A13>config>system>security>snmp#
```

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 secu-
                  rity-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 [ver-
                  sion 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
```

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** *engine-id*

Context config>system>snmp

Description This command sets the SNMP engineID to uniquely identify the SNMPv3 node. By default, the engineID is generated using information from the system backplane.

If 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.

Note: In conformance with IETF standard RFC 2274, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, 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.

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.

Ensure that the engine IDs are not used on multiple systems. A management domain can only have one instance of each engineID.

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

Default The engine ID is system generated.

Parameters *engine-id* — 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** *port-number*
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.

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 *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*]

Context config>system>security>snmp

Description 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.

Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the **community** on page 186).

Default access group configurations cannot be modified or deleted.

To remove the user group with associated, security model(s), and security level(s), use:
no access group *group-name*

To remove a security model and security level combination from a group, use:
no access group *group-name* **security-model** {**snmpv1** | **snmpv2c** | **usm**} **security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}

Default **none**

Parameters *group-name* — Specify a unique group name up to 32 characters.

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.

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.

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.

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.

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**.

context *context-name* **—** Specifies a set of SNMP objects that are associated with the context-name.

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** [*count*] [**time** *minutes1*] [**lockout** *minutes2*]
no attempts

Context config>system>security>snmp

Description 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.

If the threshold is exceeded, the host is locked out for the lockout time period.

If multiple **attempts** commands are entered, each command overwrites the previously entered command.

The **no** form of the command resets the parameters to the default values.

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 *count* — The number unsuccessful SNMP attempts allowed for the specified **time**.

Default **20**

Values 1 — 64

time *minutes1* **—** The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out.

Default **5**

Values 0 — 60

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 184 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.
- **vpls-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 *mask-value* — The mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view. (Default: all 1^{S})

The mask can be entered either:

- In hex. For example, 0xfc.
- In binary. For example, 0b11111100.

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.

type {**included** | **excluded**} **—** Specifies whether to include or exclude MIB subtree objects. *included* - All MIB subtree objects that are identified with a 1 in the mask are available in the view. (*Default: included*).

excluded - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view. (*Default: included*).

Default **included**

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** *community-string* [**hash | hash2**] **group** *group-name*
no usm-community *community-string* [**hash | hash2**]

Context config>system>security>snmp

Description 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.

Nokia'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.

The **no** form of this command removes a community string.

Default none

Parameters *community-string* — Configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used.

Values hash, hash2

group — 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*)

view

Syntax **view** *view-name* **subtree** *oid-value*
no view *view-name* [**subtree** *oid-value*]

Context config>system>security>snmp

Description 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.

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.

Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.

The **no view** *view-name* command removes a view and all subtrees.

The **no view** *view-name* **subtree** *oid-value* removes a sub-tree from the view name.

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
in packets	Displays the total number of messages delivered to SNMP from the transport service.
in gets	Displays the number of SNMP get request PDUs accepted and processed by SNMP.
in getnexts	Displays the number of SNMP get next PDUs accepted and processed by SNMP.
in sets	Displays the number of SNMP set request PDUs accepted and processed by SNMP.
out packets	Displays the total number of SNMP messages passed from SNMP to the transport service.
out get responses	Displays the number of SNMP get response PDUs generated by SNMP.
out traps	Displays the number of SNMP Trap PDUs generated by SNMP.
variables requested	Displays the number of MIB objects requested by SNMP.
variables set	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	Persistent — Persistent indexes at the last system reboot was enabled. Disabled — Persistent indexes at the last system reboot was disabled.
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	primary — Specifies whether the image was loaded from the primary location specified in the BOF. secondary — Specifies whether the image was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the image was loaded from the tertiary location specified in the BOF.
Config Source	primary — Specifies whether the configuration was loaded from the primary location specified in the BOF. secondary — Specifies whether the configuration was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the configuration was loaded from the tertiary location specified in the BOF.
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:7210 SAS E>show>system# information

===============================================================================
System Information
===============================================================================
System Name            : SAS-E
System Type            : 7210 SAS-E-1
System Version         : B-3.0.B1-44
System Contact         :
System Location        :
System Coordinates     :
System Up Time         : 31 days, 01:22:07.50 (hr:min:sec)

SNMP Port              : 161
SNMP Engine ID         : 0000197f00002889ff000000
SNMP Max Message Size  : 1500
SNMP Admin State       : Disabled
SNMP Oper State        : Disabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State        : N/A

Tel/Tel6/SSH/FTP Admin : Disabled/Disabled/Enabled/Disabled
Tel/Tel6/SSH/FTP Oper  : Down/Down/Up/Down

BOF Source             : cf1:
Image Source           : primary
Config Source          : N/A
Last Booted Config File: N/A
Last Boot Cfg Version  : N/A
Last Boot Config Header: N/A
Last Boot Index Version: N/A
Last Boot Index Header : N/A
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: Yes
User Last Modified     : admin
Time Last Modified     : 2011/03/14 00:21:55
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     : 10.135.20.137/24
Primary DNS Server     : 192.168.1.1
Secondary DNS Server   : N/A
Tertiary DNS Server    : N/A
DNS Domain             :
DNS Resolve Preference : ipv4-only
BOF Static Routes      :
  To                   Next Hop
  10.135.0.0/16        10.135.20.1

  10.135.24.0/24       10.135.20.1
  135.254.0.0/16       10.135.20.1

===============================================================================
*A:7210 SAS E>show>system#

Sample output for 7210 SAS D:

*A:SAS-D>show>system# information

===============================================================================
System Information
===============================================================================
System Name            : SAS-D
System Type            : 7210 SAS-D 6F4T-1
System Version         : B-3.0.S66
System Contact         :
System Location        :
System Coordinates     :
System Up Time         : 10 days, 01:24:01.43 (hr:min:sec)

SNMP Port              : 161
SNMP Engine ID         : 0000197f0000003f11abca11
SNMP Max Message Size  : 1500
SNMP Admin State       : Disabled
SNMP Oper State        : Disabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State        : N/A

Tel/Tel6/SSH/FTP Admin : Disabled/Disabled/Enabled/Disabled
Tel/Tel6/SSH/FTP Oper  : Down/Down/Up/Down

BOF Source             : N/A
Image Source           : primary
Config Source          : N/A
Last Booted Config File: N/A
Last Boot Cfg Version  : N/A
Last Boot Config Header: N/A
Last Boot Index Version: N/A
Last Boot Index Header : N/A
Last Saved Config      : cf1:\smitha.cfg
Time Last Saved        : 1970/01/01 00:04:11
Changes Since Last Save: Yes
User Last Modified     : admin
Time Last Modified     : 1970/01/11 00:44:21
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     : 0.0.0.0/0
Primary DNS Server     : N/A
Secondary DNS Server   : N/A
Tertiary DNS Server    : N/A
DNS Domain             :
DNS Resolve Preference : ipv4-only
BOF Static Routes      : None
===============================================================================
*A:SAS-D>show>system#
```

access-group

Syntax **access-group** *group-name*

Context show>system>security

Description This command displays access-group information.

Output **System Information Output —** The following table describes the access-group output fields.

Table 18: Show System Information 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 view to read the MIB objects.
`Write view`	Specifies the view to configure the contents of the agent.
`Notify view`	Specifies the view to send a trap about MIB objects.
`No. of access groups`	The total number of configured access groups.

Sample Output

```
A:ALA-1# 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
-------------------------------------------------------------------------------
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. 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.
`radius admin status`	The administrative status of the RADIUS protocol operation.
`tacplus admin status`	The administrative status of the TACACS+ protocol operation.

Label	Description
`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 characterisics.

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. `mgmt` — The unique SNMP community string assigned to the management router.
`View`	The view name.
`Version`	The SNMP version.
`Group Name`	The access group name.
`No of Communities`	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
===============================================================================
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-unreachble — 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.
`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.
`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`	`default` — The action to be given to the user profile if none of the entries match the command.
	`administrative` — specifies the administrative state for this profile.
`Def. Action`	`none` — No action is given to the user profile when none of the entries match the command.
	`permit-all` — The action to be taken when an entry matches the command.
`Entry`	`10 - 80` — Each entry represents the configuration for a system user.
`Description`	A text string describing the entry.

Label	Description
Match Command	administrative — Enables the user to execute all commands. configure system security — Enables the user to execute the **config system security** command. enable-admin — Enables the user to enter a special administrative mode by entering the **enable-admin** command. exec — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console. exit — Enables the user to execute the **exit** command. help — Enables the user to execute the **help** command. logout — Enables the user to execute the **logout** command. password — Enables the user to execute the **password** command. show config — Enables the user to execute the **show config** command. show — Enables the user to execute the **show** command. show system security — Enables the user to execute the **show system security** command.
Action	permit — Enables the user access to all commands. deny-all — Denies the user access to all commands.

```
A:ALA-48>config>system>snmp# show system security profile
===============================================================================
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 *oid-value* 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#
```

```
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#
```

NETCONF

In This Chapter

This chapter provides information to configure NETCONF.

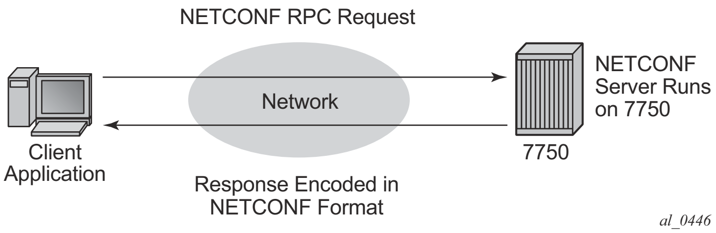
Topics in this chapter include:

NETCONF Overview

NETCONF is a standardized IETF configuration management protocol published in RFC 6241. It is secure, connection-oriented, and runs on top of the SSHv2 transport protocol as specified in RFC 6242. NETCONF can be used as an alternative to CLI or SNMP for managing an 7210 SAS OS.

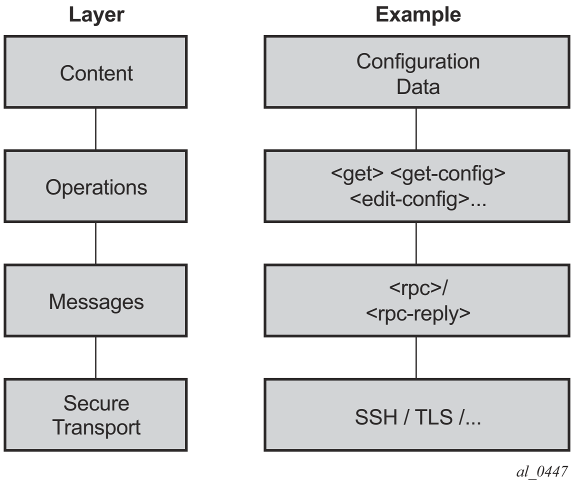
NETCONF is an XML-based protocol used to configure network devices. It uses RPC messaging for communication between a NETCONF client and the NETCONF server running on the 7210 SAS OS. An RPC message and configuration data is encapsulated within an XML document. These XML documents are exchanged between a NETCONF client and a NETCONF server in a request/response type of interaction. The 7210 SAS OS NETCONF interface supports both configuration and retrieval of operational information. Figure 4 on page 212 shows a NETCONF RPC request.

Figure 4: NETCONF RPC Request



NETCONF can be conceptually partitioned into four layers as described in RFC 6241. Figure 5 on page 212 shows the NETCONF layers.

Figure 5: NETCONF Layers (RFC 6241)



NETCONF in the 7210 SAS OS

NETCONF can be used on an 7210 SAS OS to perform router management operations including:

- Changing the configuration of the router (<edit-config> operation)

- Reading the configuration of the router (<get-config> operation, equivalent to the **info** command in the CLI)
- Reading operational status and data (and associated configuration information) (<get> operation, equivalent to the **show** commands in the CLI)

NETCONF is not used for notifications on an 7210 SAS OS; for example, log events, syslog, or SNMP notifications (traps).

The equivalent of some admin commands are available via the 7210 SAS OS NETCONF interface:

- **admin save** can be done using the <copy-config> operation
- **admin rollback** commands are supported using a CLI content layer <cli-action> RPC

The **bof**, **debug**, **tools**, and other general CLI operational commands (for example, **telnet** or **ping**) are not supported via NETCONF on an 7210 SAS OS.

The 7210 SAS OS NETCONF server advertises base capability 1.1 (in addition to 1.0).

The 7210 SAS OS supports both a CLI content layer and an XML-based content layer for NETCONF.

YANG Data Models

The 7210 SAS OS NETCONF XML content layer supports two similar proprietary configuration data models. Each configuration data model is described in a set of YANG modules. A unique set of XML namespaces is used for each of the two data models.

The YANG modules for the first configuration data model (Alcatel-Lucent Base-R13 7210 SAS OS YANG modules) have the following attributes.

- The names of the modules and submodules are alu-conf**-*-r13** (for example, alu-conf-log-r13). Note the –r13 suffix at the end of the names.
- The Nokia 7210 SAS OS YANG modules are divided into a single top-level configuration module (nokia-conf), a set of submodules (for example, nokia-conf-system) and a set of **nokia-types-*** modules. All configuration data in the Nokia 7210 SAS OS YANG modules sit in a single XML namespace urn:nokia.com:sros:ns:yang:sr:conf.
- The modules cannot be used with the <candidate> datastore.
- Although the Base-R13 modules were first introduced in 7210 SAS OS Release 13.0, they do not just contain objects from Release 13.0. Features from Release 14.0.R1, for example, are also configurable using the versions of the Base-R13 modules that are distributed with 7210 SAS OS Release 14.0.R1.

The YANG modules for the second configuration data model (Nokia SR OS YANG modules) have the following attributes.

- The names of the modules are **nokia-**conf (for example, nokia-conf-log). Note that these have no –r13 suffix in the names.
- The XML namespaces of the modules are urn:**nokia**.com:sros:ns:yang:sr:conf-* (for example, urn:nokia.com:sros:ns:yang:sr:conf-log).
- The modules can be used with the <candidate> datastore.

The two configuration data models are not interchangeable. An XML request based on the Alcatel-Lucent Base-R13 YANG modules will not work if applied to a router using the urn:**nokia**.com:sros:ns:yang:**sr**:* namespace (and vice versa).

All configuration modules and **types** modules are advertised in the 7210 SAS OS NETCONF server <hello>. Submodules are not advertized in the <hello>.

The proprietary configuration YANG data models both closely align to the 7210 SAS OS CLI configuration tree structure and commands.

The YANG modules are published and distributed as part of an 7210 SAS OS image in the cflash/support directory.

The following areas of the CLI do not have equivalent YANG data models:

- bof
- **admin**, **tools**, **debug**, or **show** branches

Transport and Sessions

SSH transport for NETCONF is supported on TCP port 830 with IPv4 or IPv6 in the Base routing instance. NETCONF SSH sessions (such as CLI, SCP and sFTP sessions) are subject to any configurable and non-configurable session limits; for example, inbound-max-sessions. Both the SSH server and NETCONF protocol must be enabled in the router configuration in order to use NETCONF. NETCONF sessions can be disconnected using the “admin disconnect” command.

NETCONF sessions do not time out automatically and are not subject to the CLI session timeout. Operators can disconnect sessions manually if they need to.

A client establishing a NETCONF session must log into the router so user accounts must exist for NETCONF on the 7210 SAS. A new access type 'netconf' is provided. For access to the Base-R13 YANG data model, both **console** and **netconf** access must be configured for the user. For access to the Nokia SR OS YANG data model, only **netconf** access is necessary.

Only authentication via the local user database is supported for NETCONF users/sessions (no RADIUS or TACACS+ authentication).

Command authorization is not supported for the Nokia 7210 SAS OS YANG configuration data model. Once a NETCONF session is established and the user is authenticated then all configuration data is available via the Nokia 7210 SAS OS YANG data model.

Command authorization is supported for the Alcatel-Lucent Base-R13 7210 SAS YANG modules. Access to various CLI config and show commands via the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules is controlled through the profile assigned to the user that is used to authenticate the underlying SSH session.

Access to LI commands using the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules is based on the **access li** configuration setting for the user.

If a NETCONF request using the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules attempts to execute a CLI command which is outside the scope of its access profile, an error response will be sent. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get>
                <filter>
                        <oper-data-format-cli-block>
                                <cli-show>system security profile </cli-show>
                        </oper-data-format-cli-block>
                </filter>
        </get>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <err-element>cli-show</err-element>
        </error-info>
        <error-message>
            command failed - 'show system security profile'
            MINOR: CLI Command not allowed for this user.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Datastores and URLs

The 7210 SAS OS supports the <running> datastore, the <candidate> datastore, the <startup> datastore, and <url> tags (**Note:** <url> is not a datastore in itself).

Support for the <candidate> datastore capability is advertised via the 7210 SAS OS NETCONF server <hello> using the urn:ietf:params:netconf:capability:candidate:1.0 capability string.

All configuration changes (<edit-config>) done to the <running> datastore via NETCONF take immediate operational effect. Configuration changes to the <candidate> datastore take effect after a successful <commit> operation.

The <startup> datastore and <url> tags can only be used with <copy-config> and <delete-config> and are not supported with any other operations (including <edit-config>, <get-config>, <get>, <validate>, etc).

The :startup capability is advertised in the 7210 SAS OS NETCONF server <hello>:

<capability>urn:ietf:params:netconf:capability:startup:1.0</capability>

The <url> tag supports the same options as CLI <file-url>: local urls (CF) and remote urls (ftp and tftp).

The :url capability is advertised in the 7210 SAS OS NETCONF server <hello>:

<capability>urn:ietf:params:netconf:capability:url:1.0?scheme=ftp,tftp,file</capability>

The following examples show the format of each URL scheme:

- <target><url>ftp://name:passwd@a.b.c.d/usr/myfiles/myfile.cfg</url></target>
- <target><url>tftp://name:passwd@a.b.c.d/usr/myfiles/myfile.cfg</url></target>
- <target><url>file:///cf3:/myfiles/myfile.cfg</url></target>
- <target><url>cf3:/myfiles/myfile.cfg</url></target>

➡ Note: The examples use “///” for the file URL. Also, the file://localhost/... format is not supported.

The <startup> datastore is identified by following the bof primary-config/secondary-config/tertiary-config paths as configured by the operator. The <startup> datastore is effectively an alias for a URL (a special URL used for system startup) with some extra resiliency (primary/secondary/tertiary).

The BOF is not considered part of any configuration datastore.

Debug configuration (such as debug mirrors, or anything saved with **admin debug-save**) is not considered part of any configuration datastore.

Lawful Interception configuration information is contained in the <running> datastore but is not saved in the <startup> datastore. The equivalent of the CLI **li save** command is available in an <edit-config> using the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules.

Configuration changes done via NETCONF are subject to CLI rollback (**revert**, **save**, and so on) and are included in the configuration when the operator performs an **admin save** in the CLI.

Only the data model described by Nokia 7210 SAS OS YANG modules can be used with the <candidate> datastore. The data model described by the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules is not applicable to the <candidate> datastore but does work with the <running> datastore. All <edit-config> requests to the candidate datastore must use the urn:nokia.com:sros:ns:yang:sr:conf namespace.

The candidate datastore supports the XML content layer only. Requests/replies to/from the candidate datastore cannot contain the CLI content layer.

NETCONF Operations and Capabilities

The following base protocol operations are supported:

- <get>
- <get-config>
- <edit-config>
- <copy-config> and <delete-config>
- <lock>
- <unlock>
- <commit>
- <discard-changes>
- <validate>

The following optional capabilities from RFC 6241 are supported:

- Writable-Running Capability

- Candidate Configuration Capability
  - <commit> operation
  - <discard-changes> operation
- Validate Capability
  - <validate> operation
- Distinct Startup Capability
- URL Capability

The following capability from RFC 6243 is supported:

- With-defaults Capability

The <edit-config> operation's <error-option> is not supported. 7210 SAS OS implements the stop-on-error behavior by default. The continue-on-error and rollback-on-error are not supported.

<get>

The CLI content layer <get> operation is supported with both configuration and state data returned in a <get> reply. An XML content layer <get> operation is supported but only configuration data is returned (no state data) in a <get> reply.

A <get> request is first analyzed for syntax errors before any execution starts. If a syntax error is found then a single global <rpc-error> for the entire request is sent in the reply.

Responses are provided for each item in the request until the first item with an error is found. The item with an error has a <response> tag containing some error information, followed by an <rpc-error> tag (and sub-tags). The reply is then returned and subsequent items are not executed.

The <rpc-error> for an individual item (i.e. for a non-syntax error) is after the </response> information and not inside the <response>.

Example — <get> request with a non-syntax error in the 2nd item:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get>
                <filter>
                        <oper-data-format-cli-block>
                                <cli-show>router interface "system"</cli-show>
                                <cli-show>router mpls lsp</cli-show>
                                <cli-show>system security ssh</cli-show>
                        </oper-data-format-cli-block>
                </filter>
        </get>
</rpc>
```

```
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <oper-data-format-cli-block>
            <item>
                <cli-show>router interface "system"</cli-show>
                <response>

===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm         Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                    PfxState
-------------------------------------------------------------------------------
system                           Up          Up/Down     Network system
   144.23.63.5/32                                                n/a
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
                </response>
            </item>
            <item>
                <cli-show>router mpls lsp</cli-show>
                <response>
                    MINOR: CLI MPLS is not configured.
                </response>
                <rpc-error>
                    <error-type>application</error-type>
                    <error-tag>operation-failed</error-tag>
                    <error-severity>error</error-severity>
                    <error-info>
                        <err-element>cli-show</err-element>
                    </error-info>
                    <error-message>
                        command failed - 'show router mpls lsp'
                    </error-message>
                </rpc-error>
            </item>
        </oper-data-format-cli-block>
    </data>
</rpc-reply>
]]>]]>
```

<get-config>

The <get-config> operation returns non-default configuration by default (i.e. the 'trim' mode as per RFC 6243).

<edit-config>

The following values for the <test-option> parameter under <edit-config> are supported:

- test-then-set
- set
- test-only

<copy-config> and <delete-config>

The <copy-config> and <delete-config> base protocol operations are supported for specific combinations of source and target datastores.

The <copy-config> operation is supported for the following combinations of sources and targets:

- <source>=<url> and <target>=<startup> (as long as both are not remote urls)
- <source>=<startup> and <target>=<url> (as long as both are not remote urls)
- <source>=<running> and <target>=<url>
  - Equivalent of “admin save <file-url>”
  - An index file is also saved if “persist on” is configured in the bof
- <source>=<running> and <target>=<startup>
  - Equivalent of “admin save”
  - An index file is also saved if “persist on” is configured in the bof

The <running> datastore cannot be a <target> for a <copy-config>.

The <candidate> datastore cannot be a <target> or a <source> for a <copy-config>.

Remote URL to remote URL copies are not supported. For example, if primary-image is a remote URL, then a <startup> to copy will fail with an error.

The <copy-config> operation uses the CLI Content Layer format. The format of the source and target is block CLI.

The <delete-config> operation is supported for the following targets:

- <url>
- <startup>

The <delete-config> operation is not allowed on the <running> or <candidate> datastore.

<lock>

Taking the <candidate> datastore’s lock is equivalent to doing a CLI exclusive transaction.

Although the NETCONF protocol allows specifying a target datastore for a lock operation, the 7210 SAS OS only implements a single lock:

- taking the running datastore’s lock locks both the running and candidate datastores (creating a single lock)
- taking the candidate datastore’s lock locks both the running and candidate datastores (creating a single lock)

When either the running datastore’s lock or the candidate datastore’s lock is taken by a NETCONF session:

- no NETCONF session can take the <running> datastore lock
- no NETCONF session can take the <candidate> datastore lock
- no other NETCONF session can do an <edit-config> on the running datastore
- no other NETCONF session can do an <edit-config> on the candidate datastore
- no other NETCONF session can do a <commit> on the candidate datastore
- no other NETCONF session can do a <discard-changes> on the candidate datastore
- the CLI becomes read-only
- **rollback revert** is blocked
- SNMP set requests fail on objects that are part of the urn:nokia.com:sros:ns:yang:sr:conf-* namespace

A datastore’s lock is unlocked when disconnecting a NETCONF session (either from the CLI using Ctrl-c, or by performing a <kill-session> or <close-session> operation). Upon disconnecting a NETCONF session that had acquired a datastore’s lock, 7210 SAS OS:

- releases the lock
- discards the “uncommitted” changes (if any)

Note: The behavior is different if the disconnected NETCONF session had the "implicit" lock (see the <edit-config> with XML Content Layer section). In that case, the 7210 SAS OS keeps the "uncommitted" changes in the <candidate> datastore.

Timeouts of locks are not supported. No specific admin/tools commands are provided to release the lock, but the session that holds the lock can be administratively disconnected using the CLI to release the lock.

From the CLI, the operator can configure whether users that belong to a specific profile have permission to lock NETCONF sessions; see the the commands.

Using CLI **show** commands, the operator can determine if either the <running> datastore's lock or the <candidate> datastore's lock is currently taken and which session has the lock; see the show commands.

<unlock>

Because there is a single lock per datastore regardless of what the scope of that lock is, the following applies.

- The <running> datastore's lock is unlocked by using the <unlock> command only on the <running> datastore. An error results and the lock stays if a different datastore is used with the <unlock> operation.
- The <candidate> datastore's lock is unlocked by using the <unlock> command only on the <candidate> datastore. An error results and the lock stays if a different datastore is used with the <unlock> operation.

Performing an <unlock> operation on the candidate datastore discards all pending (not committed) candidate datastore changes.

<commit>

The <commit> command has the following characteristics.

- It represents the equivalent of the CLI command **candidate commit**.
- When a <commit> operation fails, only the first error is returned.
- When the 7210 SAS OS cannot commit all the changes in the candidate datastore, the 7210 SAS OS keeps the <running> datastore unchanged; that is, no partial commit takes place.
- When a NETCONF session is disconnected (using Ctrl-c or <kill-session>) in the middle of a <commit> operation, 7210 SAS OS keeps the running datastore unchanged.
- The persistency of changes made via a <commit> operation is operator-controlled. A copy of the running datastore to the startup datastore is not automatically performed after each <commit> operation.
- When some changes exist in the candidate datastore (prior to being committed to the running datastore), there are some impacts to:
  - a CLI user trying to make some immediate changes, as the 7210 SAS OS blocks all CLI immediate configurations
  - an SNMP set request, as 7210 SAS OS blocks it and returns an error
  - an <edit-config> to the running datastore, as 7210 SAS OS blocks all <edit-config> requests to the running datastore and returns an error

<discard-changes>

The <discard-changes> operation causes the <candidate> datastore to revert back to match the <running> datastore and releases the "implicit" lock. From the CLI, the operator can do the equivalent of a <discard-changes> operation which releases the implicit lock as well.

<validate>

The validate:1.1 capability is supported as follows.

- The validate:1.1 and 1.0 capabilities are advertised in the NETCONF server's <hello>:
  - <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
  - <capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
- The <validate> request is supported for an XML content layer request but not for a CLI content layer request. Detection of a <config-format-cli-block> or <oper-data-format-cli-block> tag in a <validate> request will result in an "operation not supported" error response.
- A <validate> request is supported for a selection of config (<source><config>) for both the <candidate> datastore and the <running> datastore, which only returns 'OK'. The <validate> request is not supported for URL sources or the <startup> datastore.
- A <validate> operation checks mainly the syntax. Only the first error is returned.

Data Model, Datastore and Operation Combinations

Table 24 shows the which operations are supported by data model and datastore combination.

Table 24: Data Model, Datastore and Operation Combinations

Operation	R13 Modules		Nokia Modules	
	<running>	**<candidate>**	**<running>**	**<candidate>**
<edit-config>	supported	not supported	not supported	supported
<get-config>	supported	not supported	supported	supported
<get>*	retrieves CLI content layer state data (no XML content layer)		retrieves configuration data only (XML format only)	

* - Note that datastore is not applicable for a <get> operation

General NETCONF Behavior

Pressing Ctrl-c in a NETCONF session will immediately terminate the session.

The 7210 SAS OS NETCONF implementation does support XML namespaces (xmlns).

In the <rpc> element, the allowed XML namespaces are:

- the standard NETCONF "urn:ietf:params:xml:ns:netconf:base:1.0" namespace
- the 7210 SAS OS "urn:alcatel-lucent.com:sros:ns:yang:conf-r13" namespace
- the 7210 SAS OS "urn:nokia.com:sros:ns:yang:sr:conf" namespace

If any other XML namespace is declared (or assigned to a prefix) in the RPC tag, then the 7210 SAS OS returns an error.

Any prefix declarations in the rest of the request are ignored and unused. The 7210 SAS OS NETCONF server puts the correct NETCONF namespace declaration ("urn:ietf:params:xml:ns:netconf:base:1.0") in all replies.

An <edit-config> request must specify which data model (Alcatel-Lucent Base-r13 or Nokia 7210 SAS OS) is being used in the top level <configure> element.

- The 7210 SAS OS accepts a request with only a single namespace at the top <configure> element. For example:

```
<configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
   <system>
        ....
```

Or:

```
<configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
   <system>
```

- ....
- The 7210 SAS OS returns an error when a request has no namespace specified for the top <configure> node.
- The 7210 SAS OS returns an error if the request contains one or more incorrect namespaces.

Example 1 — the standard NETCONF namespace "urn:ietf:params:xml:ns:netconf:base:1.0" is used more than once in the <rpc> element:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source> <running/> </source>
<filter>
    <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
        <router>
            <interface>
               <interface-name>"system"</interface-name>
            </interface>
        </router>
    </configure>
</filter>
</get-config>
</rpc>
]]>]]>
```

Reply (no error message):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-instance>Base</router-instance>
                <interface>
                    <interface-name>system</interface-name>
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Example 2 — an allowed non-NETCONF base namespace is used in the <rpc> element:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
<get-config>
<source> <running/> </source>
<filter>
    <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
        <router>
            <interface>
              <interface-name>"system"</interface-name>
            </interface>
        </router>
    </configure>
</filter>
</get-config>
</rpc>
```

```
]]>]]>
```

Reply (non-NETCONF base namespace is allowed and no error is returned):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-instance>Base</router-instance>
                <interface>
                    <interface-name>system</interface-name>
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Example 3 — A non-standard NETCONF namespace is used in the <rpc> element:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:sr:conf">
        <get-config>
                <source><running/></source>
                <filter>
                    <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                            <router>
                                    <interface>
                                         <interface-name>"system"</interface-name>
                                    </interface>
                            </router>
                    </configure>
                </filter>
        </get-config>
</rpc>
]]>]]>
```

Reply (the 7210 SAS OS returns an error):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:sr:conf">
    <rpc-error>
        <error-type>protocol</error-type>
        <error-tag>unknown-element</error-tag>
        <error-severity>error</error-severity>
        <error-info>
          <bad-element>rpc</bad-element>
          <bad-namespace>urn:alcatel-lucent.com:sros:ns:yang:sr:conf</bad-namespace>
        </error-info>
        <error-message>
```

```
            An unexpected namespace is present.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Example 4 — a non-standard NETCONF namespace/prefix is used in one of the tags but is not defined in the <rpc> element:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source> <running/> </source>
<filter>
    <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
        <router>
            <interface xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                 <alu:interface-name>"system"</alu:interface-name>
            </interface>
        </router>
    </configure>
</filter>
</get-config>
</rpc>
]]>]]>
```

Reply (non-standard namespace/prefix used in tag is ignored):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-instance>Base</router-instance>
                <interface>
                    <interface-name>system</interface-name>
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

The chunked framing mechanism is supported (in addition to the EOM mechanism). As per RFC 6242, Section 4.1 - Framing Protocol, “[...] If the :base:1.1 capability is advertised by both peers, the chunked framing mechanism (see Section 4.2) is used for the remainder of the NETCONF session. Otherwise, the end-of-message-based mechanism (see Section 4.3) is used.”

Example 5 — Chunked message:

```
#340
<?xml version="1.0" encoding="UTF-8"?><rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><get-config><source><running/>
</source>
<filter><configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
<router><interface>
<interface-name>system</interface-name></interface></router></configure></filter>
</get-config></rpc>
##
```

Example 6 — Chunked message:

```
#38
<?xml version="1.0" encoding="UTF-8"?>
#83
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
#101
<source><running/></source>
<filter>
<configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
##39
<system>
<netconf>
</netconf>
</system>
##43
</configure>
</filter>
</get-config>
</rpc>
##
```

Handling of default data (for example, ' info' vs 'info detail') is done using the mechanisms detailed in RFC 6243. The 7210 SAS OS NETCONF server supports the 'trim' method as the default and also supports the 'report-all' method and advertises that in the <hello>:

```
 <capability>urn:ietf:params:netconf:capability:with-defaults:1.0 - basic
mode=trim&amp;also-supported=report-all</capability>
```

A user can save a rollback checkpoint (for example, prior to doing an <edit-config> or a series of <edit-config>) and perform a rollback revert if needed later using the <cli-action> RPC.

The set of supported actions are as follows:

- admin>rollback compare [to checkpoint2]
- admin>rollback compare checkpoint1 to checkpoint2
- admin>rollback delete checkpoint | rescue
- admin>rollback save [comment comment] [rescue]
- admin>rollback revert checkpoint | rescue [now]
- admin>rollback view [checkpoint | rescue]

Example 7 — Two rollback items with responses:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="102" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <cli-action>
    <admin>rollback compare active-cfg to 1</admin>
    <admin>rollback compare</admin>
  </cli-action>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="102" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <cli-action>
            <item>
                <admin>rollback compare active-cfg to 1</admin>
                <response>
            0.150 s
            0.450 s
----------------------------------------------
  configure
     router
-        mpls
-            shutdown
-            interface "system"
-                no shutdown
-            exit
-            lsp "test"
-                shutdown
-            exit
-        exit
-        rsvp
-            shutdown
-            interface "system"
-                no shutdown
-            exit
-        exit
     exit
  exit
----------------------------------------------
Finished in 0.720 s
                </response>
            </item>
            <item>
                <admin>rollback compare</admin>
                <response>
            0.160 s
            0.070 s
----------------------------------------------
  configure
     router
-        mpls
-            shutdown
-            interface "system"
-                no shutdown
-            exit
-            lsp "test"
-                shutdown
-            exit
-        exit
-        rsvp
-            shutdown
-            interface "system"
-                no shutdown
-            exit
-        exit
     exit
     service
-        vpls "99" customer 1 create
-            shutdown
-            stp
-                shutdown
-            exit
-        exit
     exit
  exit
----------------------------------------------
Finished in 0.350 s
                </response>
            </item>
        </cli-action>
    </data>
</rpc-reply>
]]>]]>
```

Example 8 — Syntax error in the request resulting in global rpc-error reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="103"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <cli-action>
      <admin>rollback compare active-cfg to 1</admin>
      <admin>rollback compare flee-fly</admin>
  </cli-action>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <err-element>admin</err-element>
        </error-info>
        <error-message>
            command failed - '/admin rollback compare flee-fly'
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Example 9 — Error processing the request:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="103"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <cli-action>
      <admin>rollback compare active-cfg to 1</admin>
      <admin>rollback compare 1 to flee-fly</admin>
  </cli-action>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <cli-action>
            <item>
                <admin>rollback compare active-cfg to 1</admin>
                <response>
            0.160 s
            0.180 s
----------------------------------------------
  configure
     router
-       mpls
-           shutdown
-           interface "system"
-               no shutdown
-           exit
-       exit
-       rsvp
-           shutdown
-           interface "system"
-               no shutdown
-           exit
-       exit
     exit
  exit
----------------------------------------------
Finished in 0.460 s
                </response>
            </item>
            <item>
                <admin>rollback compare 1 to flee-fly</admin>
                <response>
                </response>
                <rpc-error>
                    <error-type>application</error-type>
                    <error-tag>operation-failed</error-tag>
                    <error-severity>error</error-severity>
                    <error-info>
```

```
                        <err-element>admin</err-element>
                    </error-info>
                    <error-message>
                        command failed - '/admin rollback compare 1 to flee-fly'
                        MINOR: CLI No such file ('flee-fly').
                    </error-message>
                </rpc-error>
            </item>
        </cli-action>
    </data>
</rpc-reply>
]]>]]>
```

Example 10 — Error in the 2nd item of the request, resulting in no 3rd item in the reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="104" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <cli-action>
    <admin>rollback compare active-cfg to 1</admin>
    <admin>rollback compare 1 to xyz</admin>
    <admin>rollback compare active-cfg to 1</admin>
  </cli-action>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="104" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <cli-action>
            <item>
                <admin>rollback compare active-cfg to 1</admin>
                <response>
            0.170 s
            1.350 s
----------------------------------------------
  configure
     router
-       mpls
-           shutdown
-           interface "system"
-               no shutdown
-           exit
-       exit
-       rsvp
-           shutdown
-           interface "system"
-               no shutdown
-           exit
-       exit
     exit
  exit
----------------------------------------------
Finished in 1.640 s
                </response>
            </item>
            <item>
                <admin>rollback compare 1 to xyz</admin>
                <response>
                </response>
                <rpc-error>
                    <error-type>application</error-type>
                    <error-tag>operation-failed</error-tag>
                    <error-severity>error</error-severity>
                    <error-info>
                        <err-element>admin</err-element>
                    </error-info>
                    <error-message>
                        command failed - '/admin rollback compare 1 to xyz'
                        MINOR: CLI No such file ('xyz').
                    </error-message>
                </rpc-error>
            </item>
        </cli-action>
    </data>
</rpc-reply>
]]>]]>
```

System-Provisioned Configuration (SPC) Objects

There are a set of configuration objects that are provisioned (added to the <running> datastore) automatically by 7210 SAS OS; for example, log-id 99.

Some of these objects can be deleted/removed by a user (Deletable SPC Objects).

- In the CLI these are removed by specifying the keyword **no**, which is then visible in an **info** command or in a saved config (**admin save**); for example, **no log-id 99**.
- The Deletable SPC Objects can be removed or recreated via NETCONF <edit-config> requests, but they are not visible in a <get-config> response in the “urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13” namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules) when they are:
  - set to their default values (including all child leaves and objects)
  - removed or deleted
- The Deletable SPC Objects are visible in a <get-config> response in the “urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13” namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules) if a child leaf or object is changed away from the default value; for example, changing log-99 to time-format local.
- The Deletable SPC objects are visible in a <get-config> response in the “urn:nokia.com:sros:ns:yang:sr:conf” namespace (the Nokia 7210 SAS OS YANG modules) even if the child leaves are all at default values.
- The list of Deletable SPC Objects is as follows:

```
Config system security profile default
Config system security profile default entry 10-100
Config system security profile administrative
Config system security profile administrative entry 10-112
Config system security user "admin"
Config system security user console member "default"
Config system security snmp access group  xyz (a set of access groups)
Config system security ssh client-cipher-list protocol-version 1 cipher 200-210
Config system security ssh client-cipher-list protocol-version 2 cipher 190-235
Config system security ssh server-cipher-list protocol-version 1 cipher 200-205
Config system security ssh server-cipher-list protocol-version 2 cipher 190-235
Config log filter 1001
Config log filter 1001 entry 10
Config log log-id 99 & 100
```

Some SPC objects cannot be deleted (Non-Deletable SPC Objects).

- Although these objects cannot be deleted, some of them contain leaves that can be modified.
- The Non-Deletable SPC Objects are not visible in a <get-config> response in the “urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13” namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules) when they are set to their default values (including all child leaves and objects).
- The Non-Deletable SPC Objects are visible in a <get-config> response in the “urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13” namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules) if a child leaf or object is changed away from the default value; for example, setting the card-type.
- The Non-Deletable SPC objects are visible in a <get-config> response in the “urn:nokia.com:sros:ns:yang:sr:conf” namespace (the Nokia 7210 SAS OS YANG modules) even if the child leaves are all at default values.
- The list of Non-Deletable SPC Objects is as follows:

```
Config system security user-template {tacplus_default|radius_default}
Config system security snmp view iso …
Config system security snmp view li-view …
Config system security snmp view mgmt-view …
Config system security snmp view vprn-view …
Config system security snmp view no-security-view …
Config log event-control …
Config filter log 101
Config qos … various default policies can’t be deleted
Config qos queue-group-templates … these can’t be deleted
Config card <x>
Config router network-domains network-domain “default”
Config oam-pm bin-group 1
Config call-trace trace-profile “default”
```

Some Non-Deletable SPC Objects are visible in a <get-config> request in the “urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13” namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules), even if they are set to default values:

```
Config system security cpu-protection policy 254 and 255
Config router interface “system"
Config service customer 1
```

Establishing a NETCONF Session

The following example shows a client on a Linux PC initiating a connection to an 7210 SAS OS NETCONF server. The SSH session must be invoked using an SSH subsystem (as recommended in RFC 6242):

```
ssh -s my_username@a.b.c.d -p 830 netconf
```

The following example shows an exchange of hello messages which include advertisement of capabilities.

From the 7210 SAS OS server:

```
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>urn:ietf:params:netconf:base:1.0</capability>
        <capability>urn:ietf:params:netconf:base:1.1</capability>
        <capability>urn:ietf:params:netconf:capability:writable-running:1.0
        </capability>
        <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
        <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
        <capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
        <capability>urn:ietf:params:netconf:capability:startup:1.0</capability>
        <capability>urn:ietf:params:netconf:capability:url:1.0?scheme=
        ftp,tftp,file</capability>
        <capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-
        mode=trim&amp;also-supported=report-all</capability>
        <capability>urn:ietf:params:xml:ns:netconf:base:1.0?module=ietf-
        netconf&amp;revision=2011-06-01&amp;features=writable-running,validate,
        startup,url&amp;deviations=alu-netconf-deviations-r13</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:netconf-deviations-
        r13?module=alu-netconf-deviations-r13&amp;revision=2015-01-23</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-
        r13?module=alu-cli-content-layer-r13&amp;revision=2015-01-23</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-r13?module=
        alu-conf-r13&amp;revision=2016-03-11</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-aaa-r13?module=
        alu-conf-aaa-r13&amp;revision=2016-03-11</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-aa-r13?module=
        alu-conf-aa-r13&amp;revision=2016-03-11</capability>
...
        <capability>urn:nokia.com:sros:ns:yang:sr:conf?module=nokia
        -conf&amp;revision=2016-01-01</capability>
        <capability>urn:nokia.com:sros:ns:yang:sr:sros-yang-extensions?module=nokia-
        sros-yang-extensions&amp;revision=2016-01-01</capability>
        <capability>urn:nokia.com:sros:ns:yang:sr:types-eth-cfm?module=nokia-types-
        filter&amp;revision=2016-01-01</capability>
...
        <capability>urn:nokia.com:sros:ns:yang:sr:types-services?module=nokia-types-
        services&amp;revision=2016-01-01</capability>
        <capability>urn:nokia.com:sros:ns:yang:sr:types-sros?module=nokia-types
        -sros&amp;revision=2016-01-01</capability><capabilities
        <session-id>46</session-id> </hello> ]]>]]>
```

From a client:

```
<?xml version="1.0" encoding="UTF-8"?>
    <hello>
        <capabilities>
            <capability>urn:ietf:params:netconf:base:1.0</capability>
        </capabilities>
    </hello>
]]>]]>
```

XML Content Layer

XML is the default content layer format for the 7210 SAS OS NETCONF server. When using the XML format at the NETCONF content layer, configuration changes and configuration information retrieved are expressed as XML tags.

<get> with XML Content Layer

A <get> operation with an XML content layer is supported with the <candidate> datastore only. A <get> request retrieves the configuration data from the "urn:nokia.com:sros:ns:yang:sr:conf" namespace (the Nokia 7210 SAS OS YANG modules) only. If any nodes from the configure tree are included in a <get> request filter, then at minimum the <configure> tag must contain a namespace. If the namespace is not specified, the 7210 SAS OS returns errors.

Example 1: The <configure> tag contains a namespace

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get>
    <filter>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
             <python/>
        </configure>
    </filter>
</get>
</rpc>
]]>]]>
```

Reply: no errors

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <python xmlns="urn:nokia.com:sros:ns:yang:sr:conf-python">
                <python-script>
                    <script-name>testing</script-name>
                    <shutdown>false</shutdown>
                    <protection>
                    </protection>
                </python-script>
                <python-script>
                    <script-name>tested</script-name>
                    <protection>
                    </protection>
                </python-script>
            </python>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Example 2: The <configure> tag does not contain a namespace

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get>
    <filter>
        <configure>
             <python xmlns="urn:nokia.com:sros:ns:yang:sr:conf-python">
             </python>
        </configure>
    </filter>
</get>
</rpc>
]]>]]>
```

Reply: with 7210 SAS OS errors

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>protocol</error-type>
        <error-tag>unknown-element</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <bad-element>configure</bad-element>
        </error-info>
        <error-message>
            An unexpected element is present
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

<edit-config> with XML Content Layer

An <edit-config> operation is supported with the <running> datastore and the <candidate> datastore.

The <edit-config> requests to the <candidate> datastore can only write XML-formatted content.

The <edit-config> requests that specify the running datastore as a target while using the “urn:nokia.com:sros:ns:yang:sr:conf” namespace (the Nokia 7210 SAS OS YANG modules) result in an error response.

Example 1: using the <running> datastore with the urn:nokia.com:sros:ns:yang:sr:conf” namespace

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <edit-config>
          <target><running/></target>
          <config>
              <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
                  <python>
                      <python-script>
                          <script-name>testing</script-name>
                      </python-script>
                  </python>
              </configure>
          </config>
     </edit-config>
</rpc>
]]>]]>
```

Reply: with 7210 SAS OS errors

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>protocol</error-type>
        <error-tag>operation-not-supported</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <bad-element>running</bad-element>
        </error-info>
        <error-message>
            Writing to running datastore not supported in the specified namespace
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

There is an internal “implicit” lock that has a scope of all configuration commands in the 7210 SAS OS (not just the “urn:nokia.com:sros:ns:yang:sr:conf” namespace). The following actions take/release the “implicit” lock:

- the first NETCONF <edit-config> on a <candidate> datastore takes the “implicit” lock
- the completion of a NETCONF <commit> releases the “implicit” lock
- The NETCONF <discard-changes> command is supported in the 7210 SAS OS which releases the “implicit” lock as well

The following scenarios are impacted when an “implicit” lock is taken.

- A NETCONF session attempting an <edit-config> (on either the Alcatel-Lucent Base-R13 7210 SAS OS data model or the Nokia 7210 SAS OS data model) is blocked and the 7210 SAS OS replies with an error (the <error-info> element includes the <session-id> of the lock owner).
- A CLI command (on either the Alcatel-Lucent Base-R13 configuration set or the Nokia 7210 SAS OS data model) is blocked and the 7210 SAS OS returns an error.
- A SNMP set request (on objects that are part of the “urn:nokia.com:sros:ns:yang:sr:conf” namespace only) is blocked and the 7210 SAS OS returns an error.

One or more <edit-config> requests can be performed on the candidate datastore before the changes are committed or discarded.

NETCONF <edit-config> and <commit> operations impact the configuration of the router and, as with some CLI or SNMP configuration changes, additional actions or steps may need to occur before certain configuration changes take operational effect. Some examples include:

- Configuration changes that require a **shutdown** and then **no shutdown** to be performed by an operator in order to take operational effect also need this explicit **shutdown** and then **no shutdown** to be performed via NETCONF (in separate edit-configs/commits) in order to take operational effect after those configuration items are changed. Some examples include:
  - changes to Autonomous System or Confederation value require a BGP **shutdown** and then **no shutdown**
  - changes to VPRN Max-routes requires a **shutdown** and then **no shutdown** on the VPRN service
  - changes to OSPF/ISIS export-limit require a **shutdown** and then **no shutdown**on OSPF/ISIS
- Configuration changes to an msap-policy that normally require a **tools perform subscriber-mgmt eval-msap** command to take operational effect on subscribers that are already active. NETCONF can be used to change the msap-policy configuration,

but if it must have the configuration changes applied to the active subscribers then the operator must run the **eval-msap tools** command.

The supported <edit-config> operation attribute values are listed in Table 25.

Table 25: <edit-config> Operation Attribute Values

Command	Notes
urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace Alcatel-Lucent Base-R13 7210 SAS OS YANG modules	
merge (Base-R13 7210 SAS OS modules)	• For a merge operation, the operations and tags specified in an <edit-config> request are order-aware and order-dependent, and the sequence of merge operations must follow the required sequence of the equivalent CLI commands. The <edit-config> request is processed and executed in a top-down order. The same leaf can be enabled and disabled multiple times in the request and the final result is whatever was last specified for that leaf in the <edit-config> request.
remove (Base-R13 7210 SAS OS modules)	• A <remove> operation is not supported for boolean leaves. For example, any of the following example commands will return an error: – <shutdown operation="remove"/> – <shutdown operation="remove">false</shutdown> – <interface operation="remove"> <interface-name>abc</interface-name> <shutdown>true</shutdown> </interface> (For this last case <shutdown operation="merge">true</shutdown> could be used instead to make the request valid.) • A <remove> operation is the equivalent of **no** *command* in the CLI. This **no** *command* is applied whether the default for *command* is enabled (*command*), disabled (**no** *command*), or a specific value. The <remove> operation is not aware of the default value of the object or leaf being removed. • A <remove> operation for a leaf where the request also specifies a value for the leaf, will result in an error.

Table 25: <edit-config> Operation Attribute Values (Continued)

Command	Notes
delete (Base-R13 7210 SAS OS modules)	• A <delete> operation for a leaf or a presence container will not return an error if the item is already deleted. • An error is returned if attempting to delete a list node that does not exist. • A <delete> operation for a container without presence will return an error. • A <delete> operation is not supported for boolean leaves. For example, any of the following example commands will return an error: – <shutdown operation="delete"/> – <shutdown operation="delete">false</shutdown> – <interface operation="delete"> <interface-name>abc</interface-name> <shutdown>true</shutdown> </interface> (For this last case <shutdown operation="merge">true</shutdown> could be used instead to make the request valid.) • A <delete> operation is the equivalent of **no** *command* in the CLI. This **no** *command* is applied whether the default for *command* is enabled (*command*), disabled (**no** *command*), or a specific value. The <delete> operation is not aware of the default value of the object/leaf being deleted. • A <delete> operation for a leaf where the request also specifies a value for the leaf, will result in an error.
create (Base-R13 7210 SAS OS modules)	• A <create> operation for a leaf or a presence container will not return an error if the item is being set to the same value. • An error is returned if attempting to create a list node that already exists. • A <create> operation for a container without presence will result in an “OK” response (no error) but will be silently ignored. • For a <create> operation, the operations and tags specified in an <edit-config> request are order-aware and order-dependent, and the sequence of create operations must follow the required sequence of the equivalent CLI commands. The <edit-config> request is processed and executed in a top-down order. The same leaf can be enabled and disabled multiple times in the request and the final result is whatever was last specified for that leaf in the <edit-config> request.
replace (Base-R13 7210 SAS OS modules)	• not supported

Table 25: <edit-config> Operation Attribute Values (Continued)

Command	Notes
urn:nokia.com:sros:ns:yang:sr:conf namespace Nokia 7210 SAS OS YANG modules	
merge (Nokia 7210 SAS OS modules)	• supported
remove (Nokia 7210 SAS OS modules)	• A <remove> operation removes the deleted configuration and returns it to the default value. • A <remove> operation automatically removes all child objects of a deleted object (leaves, lists, containers, and so on). • Explicit shutdown of the object being removed (or any child) is not required and results in an error if a merge operation is specified on a tag that inherits a <remove> operation. • A <remove> operation is allowed on non-presence containers. The non-presence container and all of its children are removed (for example, a non-presence container with no child nodes, is not displayed in a <get> or <get-config> reply). • A <remove> operation is allowed on an object where all child branches and dependencies are automatically removed (but the <remove> operation fails if any outside objects refer to the object being removed). • A <remove> operation is allowed on a <shutdown/> leaf (which returns it to its default value). • A <remove> operation is allowed on a non-boolean leaf. • Upon specifying a <remove> operation on a node where none of its children belong to the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules), the 7210 SAS OS does not return an error and completes the node removal.

Table 25: <edit-config> Operation Attribute Values (Continued)

Command	Notes
delete (Nokia 7210 SAS OS modules)	• The 7210 SAS OS returns an error if a <delete> operation is performed on a list that does not specify a key (that is, an attempt to delete all members of a list). • The 7210 SAS OS returns an error if a <delete> operation is performed on a leaf or presence container that is already deleted (or has the default value and the default-handling is **trim**). • The 7210 SAS OS may return an error and may not complete the deletion operation when a <delete> operation is performed on a node where any of its children do not belong to the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules). • A <delete> operation removes the deleted configuration and returns it to the default value. • A <delete> operation automatically deletes all child objects of a deleted object (leaves, lists, containers, and so on). • Explicit shutdown of the object being deleted (or any of its children) is not required and results in an error if a merge operation is specified on a tag that inherits a <delete> operation. • A <delete> operation is allowed on non-presence containers. The non-presence container and all of its children are deleted (for example, a non-presence container with no child nodes is not displayed in a <get> or <get-config> reply). • A <delete> operation is allowed on an object where all child branches and dependencies are automatically deleted (but the <delete> operation fails if any outside objects refer to the object being deleted). • A <delete> operation is allowed on a <shutdown/> leaf (which returns it to its default value). • A <delete> operation is allowed on a non-boolean leaf. • Upon specifying a <delete> operation on a node where none of its children belong to the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules), the 7210 SAS OS does not return an error and completes the node deletion.
create (Nokia 7210 SAS OS modules)	• When a <create> operation for a leaf or presence container is performed, the 7210 SAS OS returns an error if the leaf or presence container is being set to the same value (unless the default-handling is **trim** and the value being set is the default value).
replace (Nokia 7210 SAS OS modules)	• not supported

The <edit-config> operation’s <default-operation> parameter is supported with the following values:

- merge
- none
  - In the urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules), an operation of “none” on a leaf node (inherited or direct) causes that leaf statement to be ignored. No error will be returned if the leaf does not exist in the data model.
  - In the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules), an operation of "none" (inherited or direct) on a leaf node that does not exist in the data model causes the 7210 SAS OS to return an error with an <error-tag> value of data-missing.

For <delete> and <remove> operations in the Nokia 7210 SAS OS namespace, the 7210 SAS OS NETCONF server will recursively “unwind” any children of the node being deleted or removed first before removing the node itself. The 'deepest' child branch of the request is examined first and any leaves are processed, after which the server works backwards out of the deepest branches back up to the object where the delete operation was specified.

For urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules), if child branches of an object are required to be removed before deleting the object in the CLI, then the equivalent delete request in a NETCONF <edit-config> request must contain all those children if they exist). For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <edit-config>
                <target><running/></target>
                <config>
                    <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                           <service>
                              <vpls operation="delete">
                                   <service-id>11</service-id>
                                    <interface>
                                        <ip-int-name>test</ip-int-name>
                                        <shutdown operation="merge">true</shutdown>
                                     </interface>
                                     <shutdown operation="merge">true</shutdown>
                               </vpls>
                            </service>
                     </configure>
                </config>
        </edit-config>
</rpc>
]]>]]>
```

In the example above, the 7210 SAS OS will first shut down the test interface, then delete the interface, then shut down the VPLS, and then finally remove it.

➡ Note: In the urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules), the 'operation="merge"' is required in the shutdown nodes; otherwise the inherited operation is delete, which is not supported on boolean leaves.

In the example above, if other children of vpls 11 exist in the config besides the interface test specified in the delete request above, and those children are required in the CLI to be deleted before removing vpls 11, then the deletion request above will fail. All configured children must be specified in the delete request.

The following applies to the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules).

- The configurations in an <edit-config> (or across multiple <edit-config> on the candidate datastore) do not need to be pre-ordered. 7210 SAS OS orders the candidate datastore configurations as needed.
- The 7210 SAS OS returns an error if an explicitly defined <edit-config> operation (such as “delete”) is specified on a “key” leaf.
- The “operation” attribute is inherited from the parent node if not explicitly specified (same as namespaces). If no parent node is available, then the “default-operation” value is used. In other words, the “operation” attribute has a “scope” that it applies to the nested nodes until it is redefined. The following scenarios simplify the “operation” inheritance, where the first line in each scenario represents the operation value of the parent node and the following lines represent the possible operation values for the child nodes and the 7210 SAS OS behavior in each case:

  1. Create

     Create/Merge: The 7210 SAS OS processes request (request succeeds/fails based on operation’s behavior)

     Delete/Remove: The 7210 SAS OS returns an error

  2. Merge

     Create/Merge/Delete/Remove: The 7210 SAS OS processes request (request succeeds/fails based on operation’s behavior)

  3. Delete/Remove

     Create/Merge: The 7210 SAS OS returns an error

     Delete/Remove: The 7210 SAS OS processes request (request succeeds/fails based on operation’s behavior)

<get-config> with XML Content Layer

A <get-config> operation is supported with the <running> datastore and the <candidate> datastore.

The <get-config> requests on the <candidate> datastore return only XML-formatted content.

On a <candidate> datastore, if no filter is specified, 7210 SAS OS returns the Nokia 7210 SAS OS configurations only.

On the <running> datastore, if no filter is specified, 7210 SAS OS returns both the Alcatel-Lucent Base-R13 configurations and the Nokia 7210 SAS OS configurations.

On the <running> datastore, to return configurations from the Alcatel-Lucent Base-R13 configurations only (or the Nokia 7210 SAS OS configurations only), the user must specify at least a top-level tag and a namespace in the filter. If the namespace is not specified, 7210 SAS OS returns an error.

The following applies to the urn:nokia.com:sros:ns:yang:sr:conf namespace (the Nokia 7210 SAS OS YANG modules):

- <get-config> requests that specify a non-existing list node or presence container result in an <rpc-error> response
- <get-config> requests that specify a list without specifying a key result in the 7210 SAS OS returning an error

Using the 'report-all' value with the <with-defaults> tag (RFC 6243) in an XML-content layer <get-config>, returns the equivalent of the CLI command **info detail** (the returned data includes attributes that are set to their default values).

Example 1: use of <with-defaults> with a value of "report-all"

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
    <source>
        <candidate/>
    </source>
    <filter>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <system>
                   <security>
                   <cpm-filter>
                        <ipv6-filter>
                        </ipv6-filter>
                        </cpm-filter>
                   </security>
</system>
        </configure>
    </filter>
    <with-defaults xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-with-defaults">
        report-all
    </with-defaults>
</get-config>
</rpc>
]]>]]>
```

Reply: returns even attributes with default values

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <system xmlns="urn:nokia.com:sros:ns:yang:sr:conf-system">
                <security>
                    <cpm-filter>
                        <ipv6-filter>
                            <shutdown>true</shutdown>
                        </ipv6-filter>
                    </cpm-filter>
                </security>
            </system>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Example 2: without using <with-defaults>

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
    <source>
        <candidate/>
    </source>
    <filter>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <system>
                   <security>
                   <cpm-filter>
                        <ipv6-filter>
                        </ipv6-filter>
                        </cpm-filter>
                   </security>
</system>
        </configure>
    </filter>
</get-config>
</rpc>
]]>]]>
```

Reply: Attributes with default values are not returned

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
```

```
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <system>
                <security>
                    <cpm-filter>
                        <ipv6-filter>
                        </ipv6-filter>
                    </cpm-filter>
                </security>
            </system>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Subtree filtering for basic subtree selection is supported for XML content layer <get-config> requests. Post-filtering of the selected subtrees is not supported.

In the urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace (the Alcatel-Lucent Base-R13 7210 SAS OS YANG modules), the subtree filtering support behaves as follows.

- Attribute match expressions (section 6.2.2 of RFC 6241) are not supported. See details below about content match nodes.
- Only containers are supported as selection nodes (section 6.2.4 of RFC 6241). Empty leaf nodes or list name nodes are not supported as selection nodes.
  - Nodes that represent lists must also include content match nodes for all keys of the list; for example, <configure><router><interface><interface-name>abc</interface-name>.
  - A selection node that is a list but does not have a key specified is not supported; for example, <configure><router><interface/> is not supported. An alternative is to request the parent containment node that contains the desired list node; for example, <configure><router> instead of <configure><router><interface/>.
- Content match nodes (section 6.2.5 of RFC 6241) are only supported for key leaves; for example, <configure><router><interface><interface-name>abc</interface-name>.
  - Content match nodes that are leaves but are not also keys will result in an error (not silently ignored).

Example 3 — A non key leaf is specified (for example, delayed-enable)

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><running/></source>
          <filter>
               <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                    <router>
                         <interface>
                              <interface-name>abc</interface-name>
                              <delayed-enable>30</delayed-enable>
                         </interface>
                    </router>
               </configure>
          </filter>
     </get-config>
</rpc>
]]>]]>
```

Reply: 7210 SAS OS errors

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>protocol</error-type>
        <error-tag>operation-not-supported</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <bad-element>delayed-enable</bad-element>
        </error-info>
        <error-message>
            Leaf element specified which is not a key.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Multiple key leafs for the same key cannot be requested inside the same instance of the list name node; for example, <interface-name>abc</interface-name> <interface-name>def</interface-name>. Each key value must be inside its own instance of the list name node; for example, <interface> <interface-name>abc</interface-name> </interface> <interface> <interface-name>def</interface-name> </interface>.

Example 4 — A valid <get-config> request (content match on a list key):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-config>
        <source>
            <running/>
        </source>
       <filter>
            <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                    <router>
                        <interface>
                                <interface-name>abc</interface-name>
                        </interface>
                    </router>
            </configure>
       </filter>
        </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-instance>Base</router-instance>
                <interface>
                    <interface-name>abc</interface-name>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Example 5 — A valid <get-config> request (selection node that is a container):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-config>
        <source>
            <running/>
        </source>
        <filter>
                <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                        <router/>
                </configure>
        </filter>
    </get-config>
</rpc>
]]>]]>
```

The reply will contain all the configuration for all child nodes of config>router

Example 6 — An invalid <get-config> request (list name node - invalid selection node):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><running/></source>
          <filter>
               <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                    <router>
                         <interface>
                         </interface>
                    </router>
               </configure>
          </filter>
     </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <err-element>get-config</err-element>
        </error-info>
        <error-message>
            command failed - 'configure router interface'
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Example 7 — An invalid <get-config> request (empty leaf node - invalid selection node):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get-config>
            <source>
                <running/>
            </source>
            <filter>
                <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                    <system>
                            <security>
                                        <ftp-server>
                                        </ftp-server>
                             </security>
                    </system>
                 </configure>
            </filter>
        </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>protocol</error-type>
        <error-tag>operation-not-supported</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <bad-element>ftp-server</bad-element>
        </error-info>
        <error-message>
            Leaf element specified which is not a key.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

Example 8 — An invalid <get-config> request (key repeated in the same instance of the list node):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get-config>
                <source>
                        <running/>
                </source>
                <filter>
                        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-
r13">
                                <router>
                                        <interface>
                                                <interface-name>abc</interface-name>
                                                <interface-name>def</interface-name>
                                        </interface>
                                </router>
                        </configure>
                </filter>
        </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <err-element>get-config</err-element>
        </error-info>
        <error-message>
            command failed - 'configure router interface "abc" "def"'
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

The full configuration (equivalent to the CLI command 'admin display-config') can be obtained via a <get-config> request:

- A — when the <filter> tag is not present

  For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><running/></source>
     </get-config>
</rpc>
]]>]]>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><candidate/></source>
     </get-config>
</rpc>
]]>]]>
```

- B — when only the <configure> tag is present inside a <filter> tag

  For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><running/></source>
          <filter>
               <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13"/>
          </filter>
     </get-config>
</rpc>
]]>]]>

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <get-config>
          <source><candidate/></source>
          <filter>
               <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf"/>
          </filter>
     </get-config>
</rpc>
]]>]]>
```

The <get-config> requests that specify a non-existent list node or presence container will result in a reply that contains no data for those list nodes or containers. An rpc-error is not sent in this case.

XML Content Layer Examples

The following examples can be used after a NETCONF session has been established including the exchange of the <hello> messages.

Below is an example of a <get-config> request on the <running> datastore to check on whether netconf is shut down or not on the router:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get-config>
                <source> <running/> </source>
                <filter>
                        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-
```

```
r13">
                                <system>
                                        <netconf>
                                        </netconf>
                                </system>
                        </configure>
                </filter>
        </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <system>
                <netconf>
                    <shutdown>false</shutdown>
                </netconf>
            </system>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Below is an example for a <get-config> request on the <candidate> datastore to get the full configurations of the system, qos and log branches:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
    <source><candidate/></source>
    <filter>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
           <system>
           </system>
        </configure>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <qos>
            </qos>
        </configure>
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <log/>
        </configure>
    </filter>
</get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
```

```
        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
            <system>
                <contact>tester</contact>
                <name>r2-node</name>
                <location>over-here</location>
                <lldp>
                    <shutdown>false</shutdown>
                </lldp>
...
...
</system>
            <qos>
                <sap-ingress>
                    <policy-id>1</policy-id>
                    <policy-name>default</policy-name>
                    <description>Default SAP ingress QoS policy.</description>
                    <sub-insert-shared-pccrule>
                    </sub-insert-shared-pccrule>
                    <dynamic-policer>
                        <range>
                        </range>
                        <parent>
                        </parent>
                    </dynamic-policer>
                    <mac-criteria>
                    </mac-criteria>
                    <ip-criteria>
                    </ip-criteria>
                    <ipv6-criteria>
                    </ipv6-criteria>
...
...
                </sap-egress>
            </qos>
            <log>
                <route-preference>
                </route-preference>
                <app-route-notifications>
                </app-route-notifications>
                <event-control>
                    <application-id>1</application-id>
                    <event-number>4401</event-number>
                    <severity-level>major</severity-level>
                    <throttle>true</throttle>
                </event-control>
...
...
</log>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

Below is an example of an <edit-config> request om the <running> datastore to create a basic VPRN service:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
```

```
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <edit-config>
       <target>
            <running/>
        </target>
        <config>
            <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                <service>
                    <vprn operation="create">
                        <service-id>200</service-id>
                        <customer>1</customer>
                    </vprn>
                </service>
            </configure>
        </config>
  </edit-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
]]>]]>
```

Below is an example of an <edit-config> request on the <candidate> datastore to create a basic epipe service:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <edit-config>
        <target><candidate/></target>
        <config>
                        <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
                                <service>
                                        <epipe>
                                                <service-id>444</service-id>
                                                <customer>1</customer>
                                                <service-mtu>1514</service-mtu>
                                        </epipe>
                                </service>
                        </configure>
        </config>
        </edit-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
]]>]]>
```

Below is an example of a <edit-config> request on the <running> datastore to create a basic VPRN service with a SAP (creates the service/interface but fails to create the SAP as the specified port's encapsulation is invalid):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <edit-config>
                <target>
            <running/>
        </target>
        <config>
            <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                <service>
                    <vprn operation="create">
                        <interface>
                            <ip-int-name>"test"</ip-int-name>
                            <sap>
                                <sap-id>"2/1/1"</sap-id>
                            </sap>
                        </interface>
                        <service-id>201</service-id>
                        <customer>1</customer>
                    </vprn>
                </service>
            </configure>
        </config>
  </edit-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <err-element>edit-config</err-element>
        </error-info>
        <error-message>
            command failed -
 'configure service vprn "201" customer 1 interface "test" sap "2/1/1"'
            MINOR: CLI SAP-id has an invalid port number or encapsulation value.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

CLI Content Layer

When using the CLI format at the NETCONF content layer, configuration changes and configuration information retrieved are expressed as untagged (non-XML) CLI commands; for example, CLI script.

The script must be correctly ordered and has the same dependencies and behavior as CLI. The location of CR/LF (ENTER) within the CLI for an <edit-config> is significant and affects the processing of the CLI commands, such as what CLI branch is considered the “working context”. In the following two examples, the “working context” after the commands are issued are different.

Example 1:

```
exit all  [<-ENTER]
configure system time zone EST [<-ENTER]
```

Example 2:

```
exit all [<-ENTER]
configure  [<-ENTER]
    system  [<-ENTER]
        time  [<-ENTER]
            zone EST [<-ENTER]
```

After example 1, the CLI working context is the root and immediately sending 'dst-zone CEST' would return an error. After example 2, the CLI working context is config>system>time and sending 'dst-zone CEST' would work as expected.

Configuration changes done via NETCONF trigger the same “change” log events (for example, tmnxConfigCreate) as a normal CLI user doing the same changes.

The <with-defaults> tag (RFC 6243) is not supported in a CLI content layer request.

The operator can get a full configuration including defaults for a CLI Content Layer using an empty <cli-info-detail>. The full configuration (equivalent to the CLI command 'admin display-config [detail]') can be obtained via a <get-config> request in a CLI Content Layer format with an empty <cli-info> or <cli-info-detail> tag inside a <config-format-cli-block>. <report-all> is not supported.

Post-processing commands are ignored: "| match" (pipe match), "| count" (pipe count) and ">" (redirect to file) and CLI ranges are not supported for any command; for example, show card [1..5].

CLI Content Layer Examples

The following examples can be used after a NETCONF session has been established including the exchange of the <hello> messages.

The following shows an example of a configuration change request and response.

Note: The **exit all** command is not required at the beginning of the CLI block; it is automatically assumed by the 7210 SAS OS NETCONF server.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="104" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <edit-config>
    <target><running/></target>
        <config>
            <config-format-cli-block>
                configure system
                    time zone EST
                    location over-here
                exit all
            </config-format-cli-block>
        </config>
    </edit-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="104"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
]]>]]>
```

The following is an example of a <get-config> request and response to retrieve configuration information:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-config>
        <source>
            <running/>
        </source>
        <filter>
            <config-format-cli-block>
                <cli-info>router</cli-info>
                <cli-info-detail>system login-control</cli-info-detail>
            </config-format-cli-block>
        </filter>
    </get-config>
```

```
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <config-format-cli-block>
            <item>
                <cli-info>router</cli-info>
                <response>
----------------------------------------------
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
        interface "system"
            no shutdown
        exit
----------------------------------------------
                </response>
            </item>
            <item>
                <cli-info-detail>system login-control</cli-info-detail>
                <response>
----------------------------------------------
            ftp
                inbound-max-sessions 3
            exit
            ssh
                no disable-graceful-shutdown
                inbound-max-sessions 5
                outbound-max-sessions 5
                no ttl-security
            exit
            telnet
                no enable-graceful-shutdown
                inbound-max-sessions 5
                outbound-max-sessions 5
                no ttl-security
            exit
            idle-timeout 30
            no pre-login-message
            no motd
            login-banner
            no exponential-backoff
----------------------------------------------
                </response>
            </item>
        </config-format-cli-block>
    </data>
</rpc-reply>
]]>]]>
```

The following example shows a <get-config> request and response to retrieve full configuration information.

Note: The <cli-info-detail/> request can be used to get the full configuration, including default settings.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <get-config>
          <source>
               <running/>
          </source>
          <filter>
              <config-format-cli-block>
                  <cli-info/>
              </config-format-cli-block>
          </filter>
    </get-config>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <config-format-cli-block>
            <item>
                <cli-info></cli-info>
                <response>
# TiMOS-C-0.0.I4301 cpm/x86_64 ALCATEL SR 7750 Copyright (c) 2000-2015 Alcatel-Lucent.
# All rights reserved. All use subject to applicable license agreements.
# Built on Sun Jan 4 19:11:11 PST 2015 by builder in /rel0.0/I4301/panos/main

# Generated WED JAN 07 01:07:43 2015 UTC

exit all
configure
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        chassis-mode d
        dns
        exit
        load-balancing
            lsr-load-balancing lbl-ip
            system-ip-load-balancing
        exit
        netconf
            no shutdown
        exit
        snmp
            shutdown
            engineID "deadbeefdeadbeef"
        exit
        time
            ntp
```

```
                authentication-key 1 key "OAwgNUlbzgI" hash2 type des
                no shutdown
            exit
            sntp
                shutdown
            exit
            zone EST
        exit
        thresholds
            rmon
            exit
        exit
#--------------------------------------------------
echo "Cron Configuration"
#--------------------------------------------------
        cron
            ...
            ...
            ...
        exit
    exit
#--------------------------------------------------
echo "System Security Configuration"
#--------------------------------------------------
    ...
    ...
    ...
#--------------------------------------------------
echo "System Time NTP Configuration"
#--------------------------------------------------
    system
        time
            ntp
            exit
        exit
    exit

exit all

# Finished WED JAN 07 01:07:43 2015 UTC
----------------------------------------------
----------------------------------------------
                </response>
            </item>
        </config-format-cli-block>
    </data>
</rpc-reply>
]]>]]>
```

The following is an example of a <get> request and the response to it:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get>
        <filter>
            <oper-data-format-cli-block>
                <cli-show>system security ssh</cli-show>
            </oper-data-format-cli-block>
        </filter>
    </get>
</rpc>
]]>]]>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
        <oper-data-format-cli-block>
            <item>
                <cli-show>system security ssh</cli-show>
                <response>

===============================================================================
SSH Server
===============================================================================
Administrative State      : Enabled
Operational State         : Up
Preserve Key              : Enabled

SSH Protocol Version 1    : Disabled

SSH Protocol Version 2    : Enabled
DSA Host Key Fingerprint  : ca:ce:37:90:49:7d:cc:68:22:b3:06:2c:11:cd:3c:8e
RSA Host Key Fingerprint  : 49:7c:21:97:42:35:83:61:06:95:cd:a8:78:4c:1e:76

-------------------------------------------------------------------------------
Connection                                Username
    Version Cipher                        ServerName  Status
-------------------------------------------------------------------------------
135.121.143.254                           admin
    2       aes128-cbc                    netconf     connected
-------------------------------------------------------------------------------
Number of SSH sessions : 1
===============================================================================
                </response>
            </item>
        </oper-data-format-cli-block>
    </data>
</rpc-reply>
]]>]]>
```

NETCONF Command Reference

Command Hierarchies

Configuration Commands

This section provides the NETCONF configuration command reference. Topics in this section include:

Netconf System Commands

```
config
    — system
        — netconf
            — [no] shutdown
```

Netconf Security Commands

```
config
    — system
        — security
            — profile profile-id
                — netconf
                    — base-op-authorization
                        — [no] kill-session
```

SHOW COMMANDS

```
show
    — system
        — netconf
            — counters
```

Configuration Commands

This section provides NETCONF configuration command descriptions.

NETCONF System Commands

shutdown

Syntax **[no] shutdown**

Context config>system>netconf

Description This command disables the NETCONF server. The shutdown command is blocked if there are any active NETCONF sessions.   Use the admin disconnect command to disconnect all NETCONF sessions before shutting down the NETCONF service.

NETCONF Security Commands

netconf

Syntax **netconf**

Context config>system>security>profile

Description This command authorizes netconf capability for the user.

base-op-authorization

Syntax **base-op-authorization**

Context config>system>security>profile>netconf

Description This command enables the context where permission to use various NETCONF operations is controlled.

kill-session

Syntax **[no] kill-session**

Context config>system>security>profile>netconf>base-op-authorization

Description This operation authorizes a user associated with the profile to send a kill session NETCONF operation. This kill session operation allows a NETCONF client to kill another NETCONF session, but not the session in which the operation is requested.

Default no kill-session

Show Command

netconf

Syntax **netconf**

Context show>system

Description This command displays NETCONF SSH sessions.

Table 26 describes the NETCONF output fields.

Show System NETCONF Output Fields

Table 26: Show System NETCONF Output Fields

Label	Description
`Administrative State`	Enabled Displays that NETCONF is enabled. Disabled Displays that NETCONF is disabled.
`Operational State`	Up Displays that NETCONF is operational. Down Displays that NETCONF is not operational.
`Connection`	The IP address of the connected router(s) (remote client).

```
7210SAS>show>system# netconf
```

```
===============================================================================
NETCONF Server
===============================================================================
Administrative State      : Disabled
Operational State         : Down
===============================================================================
7210SAS>show>system#
```

counters

Syntax **counters**

Context show>system>netconf

Description This command displays NETCONF counters.

Table 27 describes the NETCONF counter output fields.

NETCONF Counters Output Fields

Table 27: NETCONF Counters Output Fields

Label	Description
RX Messages	Types and numbers of received messages
RX Total	Total of all received messages
TX Messages	Types and numbers of sent messages
TX Total	Total of all sent messages
failed edit-configs	Number of failed <edit-config> requests due to a lock (including implicit ones) being taken by other netconf sessions
failed locks	Number of failed <lock> requests due to a lock (including implicit ones) being taken by other netconf sessions

Sample

```
7210SAS>show>system# netconf counters
==============================================================================
NETCONF counters:
==============================================================================
    Rx Messages
------------------------------------------------------------------------------
      in gets           : 0
      in get-configs    : 0
      in edit-configs    : 0
      in copy-configs    : 0
      in delete-configs  : 0
      in validates       : 0
      in close-sessions  : 0
      in kill-sessions   : 0
------------------------------------------------------------------------------
      Rx Total           : 0
==============================================================================
    Tx Messages
------------------------------------------------------------------------------
      out rpc-errors     : 0
------------------------------------------------------------------------------
      Tx Total           : 0
==============================================================================

7210SAS>show>system#
```

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

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 infomation.

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 28.

Table 28: 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 . Accounting statistics are collected by counters for individual service 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 274
- Session on page 274
- Memory Logs on page 274
- Log Files on page 275
- SNMP Trap Group on page 277
- Syslog on page 277

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.

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)

Accounting log files are created in the **\act-collect** directory on a compact flash device (*cf1*). 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 aaff-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 29 displays the severity level mappings to syslog severities.

Table 29: 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 6 depicts a function block diagram of event logging.

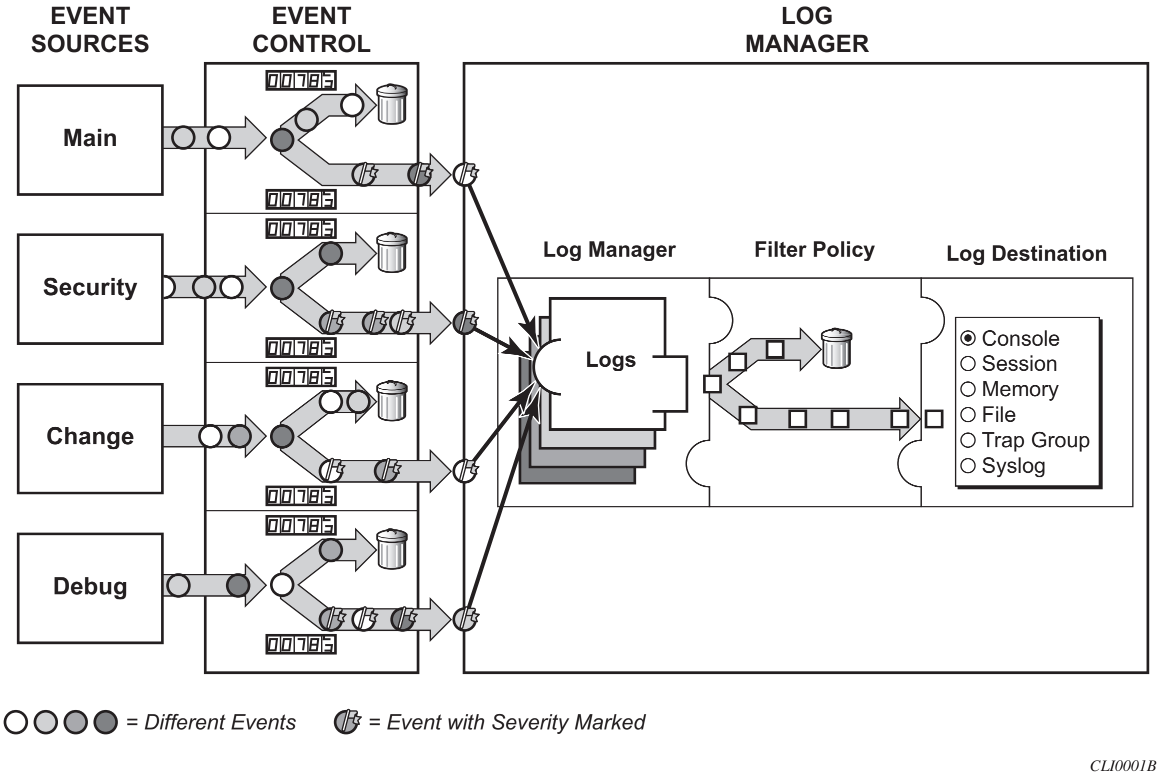


Figure 6: Event Logging Block Diagram

Event Sources

In Figure 6, 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 7 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
SVCMGR
SYSTEM
TIP
TOD
USER
VRTR
==================================
*A:ALU-7210#
```

Figure 7: 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 287.

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 vRtrIgmpIfRxQueryVerMismatch    WA  gen          0           0
   2002 vRtrIgmpIfCModeRxQueryMismatch  WA  gen          0           0
   2003 vRtrIgmpMaxGrpsLimitExceeded    WA  gen          0           0
   2004 vRtrIgmpMcacPlcyDropped         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
...
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 30:

Table 30: 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 31.

Table 31: Log Entry Field Descriptions

Label	Description
`nnnn`	The log entry sequence number.
`YYYY/MM/DD`	The UTC date stamp for the log entry. *YYYY* — Year *MM* — Month *DD* — Date
`HH:MM:SS.SS`	The UTC time stamp for the event. *HH* — Hours (24 hour format) *MM* — Minutes *SS.SS* — Seconds
`<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).

Table 31: Log Entry Field Descriptions (Continued)

Label	Description
`<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 (*cf1:*) 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 service and network accounting policies are shown below.

Accounting Record Names for 7210 SAS-D

Table 32: Accounting Record Name and Collection Periods (for 7210 SAS-D devices)

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
service-ingress-octets	sio	Access SAP	5
service-egress-octets	seo	Access SAP	5
service-ingress-packets	sip	Access SAP	5
service-egress-packets	sep	Access SAP	5
combined-service-ingress	sip, sio	Access SAP	5
combined-service-egress	seo, sep	Access SAP	5
complete-service-ingress-egress	sip, sio, seo, sep	Access SAP	5
access-egress-packets	aep	Access-port	5
access-egress-octets	aeo	Access-port	5
combined-access-egress	cmAeo, cmAep	Access-port	5
network-ingress-octets	nio	Access-uplink-port	15
network-ingress-packets	nip	Access-uplink-port	15
network-egress-octets	neo	Access-uplink-port	15
network-egress-packets	neo	Access-uplink-port	15
combined-network-egress	cmNeo, cmNep	Access-uplink-port	15
combined-network-ingress-egress-octets	cmNio, cmNeo	Access-uplink-port	15

Accounting Record Names for 7210 SAS-E

Table 33: Accounting Record Name and Collection Periods (for 7210 SAS-E devices)

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
service-ingress-octets	sio	Access SAP	5
service-ingress-packets	sip	Access SAP	5
network-ingress-octets	nio	network port	15
network-ingress-packets	nip	network port	15
service-egress-pkts	sep	Access SAP	5
combined-service-ingress-egress-pkts	cmSip & cmSep	Access SAP	5
access-egress-packets	aep	access port	5
network-egress-packets	nep	Access-uplink-port	15
combined-network-ingress-egress-pkts	cmNip & cmNep	Access-uplink-port	15

Accounting Records for 7210 SAS-K2F2T1C

Table 34: Accounting Record Name and Collection Periods (7210 SAS-K2F2T1C devices)

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
service-ingress-octets	sio	Access SAP	5
service-egress-octets	seo	Access SAP	5
service-ingress-packets	sip	Access SAP	5
service-egress-packets	sep	Access SAP	5
combined-service-ingress	sip, sio	Access SAP	5
combined-service-egress	seo, sep	Access SAP	5
complete-service-ingress-egress	sip, sio, seo, sep	Access SAP	5
network-ingress-octets	nio	Access-uplink-port	15
network-ingress-packets	nip	Access-uplink-port	15
network-egress-octets	neo	Access-uplink-port	15
network-egress-packets	neo	Access-uplink-port	15
combined-network-egress	cmNeo, cmNep	Access-uplink-port	15
combined-network-ingress-egress-octets	cmNio, cmNeo	Access-uplink-port	15

Accounting Records for 7210 SAS-K2F4T6C

Table 35: Accounting Record Name and Collection Periods (7210 SAS-K 2F4T6C devices)

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
service-ingress-octets	sio	Access SAP	5
service-egress-octets	seo	Access SAP	5
service-ingress-packets	sip	Access SAP	5
service-egress-packets	sep	Access SAP	5
combined-service-ingress	sip, sio	Access SAP	5
combined-service-egress	seo, sep	Access SAP	5
complete-service-ingress-egress	sip, sio, seo, sep	Access SAP	5
combined-access-egress	cmAeo, cmAep	Access-port	5
network-ingress-octets	nio	Access-uplink-port and Network port	15
network-ingress-packets	nip	Access-uplink-port and Network port	15
network-egress-octets	neo	Access-uplink-port and Network port	15
network-egress-packetss	neo	Access-uplink-port and Network port	15
combined-network-egress	cmNeo, cmNep	Access-uplink-port and Network port	15
combined-network-ingress-egress-octets	cmNio, cmNeo	Access-uplink-port and Network port	15
saa (supported only on 7210 SAS-D, 7210 SAS-E, and 7210 SAS-K 2F2T1C)			5
complete-pm (supported only on 7210 SAS-K 2F4T6C)			5

When creating accounting policies, one service accounting policy and one network accounting policy can be defined as default. If statistics collection is enabled on a SAP, access-uplink, or network port and no accounting policy is applied, then the respective default 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 in turn composed of multiple fields. Table 34, Table 35, and Table 36 lists the accounting policy record names and the statistics collected.

Accounting Record Details for 7210 SAS-E

Table 39: Accounting Record Name Details (for 7210 SAS-E devices)

Record Name	Sub-Record	Field	Field Description
Service-ingress-octets (sio) (**) (counter mode is **in-out-profile-count**)	sio	svc	SvcId
		sap	SapId
		mid	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
Service-ingress-octets (counter mode is **forward-drop-count**)	sio	svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
Service-ingress-packets (sip) (*) (**) (counter mode is **in-out-profile-count**)	sip	svc	SvcId
		sap	SapId
		mid	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded

Record Name	Sub-Record	Field	Field Description
Service-ingress-packets (counter mode is **forward-drop-count**)	sip	svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		p	PacketsDropped
Network-ingress-octets (nio)	nio	port	PortId
		mid	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
Network-ingress-packets (nip)	nip	port	PortId
		mid	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
Service-egress-pkts (sep) (*) (**)	sep	svc	SvcId
		sap	SapId
		epf	PacketsForwarded
Combined-service-ingress-egress-pkts (counter mode is **in-out-profile-count**)	cmSip cmSep	svc	SvcId
		sap	SapId
		epf	PacketsForwarded
		ipo	PacketsReceived
		mid	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
Combined-service-ingress-egress-pkts(counter mode is **forward-drop-count**)	cmSip, cmSep	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		of	OctetsForwarded
		od	OctetsDropped
		epf	PacketsForwarded
Access-egress-packets	aep	port	PortId
		qId	QueueId
		epf	PacketsForwarded
Network-egress-packets	nep	port	PortId
		qId	QueueId
		epf	PacketsForwarded

Record Name	Sub-Record	Field	Field Description
Combined-network-ingress-egress-packets	cmNip cmNep	port	PortId
		mid	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		qld	QueueId
		epf	PacketsForwarded

Accounting Record Details for 7210 SAS-D

Table 40: Accounting Record Name Details (for 7210 SAS-D devices)

Record Name	Sub-Record	Field	Field Description
		(Per Meter)	(Per Meter)
Service-ingress-octets (counter mode is **in-out-profile-count**)	sio	svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered

Record Name	Sub-Record	Field	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
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)
		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	IngressPktsOffered
Service-ingress-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	IngressPktsOffered

Record Name	Sub-Record	Field	Field Description
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)
		svc	SvcId
		sap	SapId
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		pf	PktsForwarded
		pd	PktsDropped
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)
	seo, sep	svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
Combined-service-ingress(counter mode is **forward-drop-count**)	sip, sio	(Per Meter)	(Per Meter)
		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

Record Name	Sub-Record	Field	Field Description
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)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
		(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)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePktsFOrwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
	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
		pd	PktsDropped

Record Name	Sub-Record	Field	Field Description
Complete-service-ingress-egress(counter mode is " forward-drop-count") **NOTE**: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	sip sio	(Per Meter)	(Per Meter)
		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
		(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
		pd	PktsDropped
Access-egress-octets	aoe	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Access-egress-packets	aep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped

Record Name	Sub-Record	Field	Field Description
Combined-access-egress	cmAeo, cmAep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForawrded
		pf	PktsForwarded
		pd	PktsDropped
		od	OctetsDropped
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
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	Octets Dropped

Record Name	Sub-Record	Field	Field Description
Combined-network-ing-egr-octets	cmNio, cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped

Accounting Record Details for 7210 SAS-K2F2T1C

Table 41: Accounting Record Details (for 7210 SAS-K2FT1C devices)

Record Name	Sub-Record	Field	Field Description
		(Per Ingress queue)	(Per Ingress queue)
Service-ingress-octets	sio	svc	SvcId
		sap	SapId
		qid	Queue Id
		iof	InProfileOctetsForwarded
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded

Record Name	Sub-Record	Field	Field Description
Service-ingress-packets	sip	(Per Ingress queue)	(Per Ingress queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPacketsOffered
Service-egress-packets	sep	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Queue Id
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPacketsForwarded

Record Name	Sub-Record	Field	Field Description
Combined-service-ingress	sio, sip	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
combined-service-egress	seo sep	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded

Record Name	Sub-Record	Field	Field Description
complete-service-ingress-egress	sio sip	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
	seo sep	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded
network-ingress-octets	nio	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped

Record Name	Sub-Record	Field	Field Description
network-egress-octets	neo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
network-ingress-Packets	nip	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		opd	OutprofilePacketsDropped
network-egress-Packets	nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		od	OctetsDropped
		opd	OutprofilePacketsDropped
combined-network-egress	cmNeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
		iod	InprofileOctetsDropped
	cmNep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		opd	OutprofilePacketsDropped

Record Name	Sub-Record	Field	Field Description
combined-network-ing-egr-octets	cmNio	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
	cmNeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped

Accounting Record Details for 7210 SAS-K2F4T6C

Table 42: Accounting Record Name Details (for 7210 SAS-K2F4T6C devices)

Record Name	Sub-Record	Field	Field Description
		(Per Ingress queue)	(Per Ingress queue)
Service-ingress-octets	sio	svc	SvcId
		sap	SapId
		qid	Queue Id
		iof	InProfileOctetsForwarded
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded

Record Name	Sub-Record	Field	Field Description
Service-ingress-packets	sip	(Per Ingress queue)	(Per Ingress queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPacketsOffered
Service-egress-packets	sep	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Queue Id
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPacketsForwarded

Record Name	Sub-Record	Field	Field Description
Combined-service-ingress	sio, sip	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
combined-service-egress	seo sep	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded

Record Name	Sub-Record	Field	Field Description
complete-service-ingress-egress	sio sip	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Ingress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
	seo sep	(Per Queue)	(Per Queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		iof	Forwarded InProfile Octets
		oof	Forwarded OutProfile Octets
		iod	Dropped InProfile Octets
		ood	Dropped OutProfile Octets
		ipf	Forwarded InProfile Packets
		opf	Forwarded OutProfile Packets
		ipd	Dropped InProfile Packets
		opd	Dropped OutProfile Packets
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded
network-ingress-octets	nio	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped

Record Name	Sub-Record	Field	Field Description
network-egress-octets	neo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
network-ingress-Packets	nip	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		opd	OutprofilePacketsDropped
network-egress-Packets	nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		od	OctetsDropped
		opd	OutprofilePacketsDropped
combined-network-egress	cmNeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
		iod	InprofileOctetsDropped
	cmNep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		ipf	InProfilePacketsForwarded
		ipd	InprofilePacketsDropped
		opf	OutProfilePacketsForwarded
		opd	OutprofilePacketsDropped

Record Name	Sub-Record	Field	Field Description
combined-network-ing-egr-octets	cmNio	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
	cmNeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		iof	InProfileOctetsForwarded
		iod	InprofileOctetsDropped
		oof	OutProfileOctetsForwarded
		ood	OutprofileOctetsDropped
combined-sdp-ingress egress	cmSdpipo	svc	svcID
		sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo	svc	svcID
		sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
complete-sdp-ingress-egress	cmSdpipo	svc	svcID
		sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo	svc	svcID
		sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo	sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo	sdp	sdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

Configuration Guidelines

1. In 7210 SAS-E devices, the ingress SAP counter operates in either octet or packet mode when either in-out-profile-count or forward-drop-count is in use. The mode of the counter can be configured to collect data in either packets or octets. The counter mode can be specified for ingress SAP counters only. The egress SAP counters collect only the number of packets. The accounting records collect the packet or octet count on a SAP based on the accounting policy associated with the SAP. The default mode of the ingress SAP counter is set to packet.
2. In 7210 SAS-D device, the ingress SAP counter counts both octets and packets simultaneously.
3. For 7210 SAS-D and 7210 SAS-E devices, the egress SAP counter is disabled by default.
4. In 7210 SAS-E, the mode of the counter cannot be changed if an accounting policy is already associated with a SAP.
5. Ensure that egress SAP counters are enabled on 7210 SAS-E devices before associating accounting records of type Service-egress-pkts and Combined- service-ingress-egress-pkts.
6. Ensure that egress SAP counters are enabled on 7210 SAS-D devices before associating accounting records of type Service-egress-octets, service-egress-packets,combined-service-egress and complete-service-ingress-egress
7. Before modifying the counter mode, 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.
8. Egress SAP statistics are not available on any of the SAPs of a port, on which a dot1q SAP and dot1q default SAP configuration are present at the same time.
9. In 7210 SAS-D and E devices for VLL and VPLS services, the counter-mode of counters associated with SAP ingress meters/policers can be changed by executing the following command:
   - config>service>epipe/vpls>sap>statistics>ingress>counter-mode {in-out-profilecount| forward-drop-count}. (For 7210 SAS-D devices)
   - config>service>epipe/vpls>sap>statistics>ingress>counter-mode {packet | octet}{inout-profile-count|forward-drop-count}. (For 7210 SAS-E devices)
     For more information on the counter-mode command refer to the 7210 SAS E,D Services guide.
10. The statistics collected for the following accounting records listed below vary based on the counter-mode selected:
    - Service-ingress-octets
    - Service-ingress-packets
    - Combined-service-ingress
    - Complete-service-ingress-egress

Table 28, Table 29, and Table 34 above depicts the changes in the records based on the counter-mode selected.

Reporting and Time-Based Accounting

Node support for volume and time-based accounting concept provides an extra level of intelligence at the network element level in order to provide service models such as “prepaid access” in a scalable manner. This means that the network element gathers and stores per-subscriber accounting information and compare it with “pre-defined” quotas. Once a quota is exceeded, the pre-defined action (such as re-direction to a web portal or disconnect) is applied.

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

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 service access points (SAPs), access-uplink(network) ports, and access ports .
- 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 322
- Configuring an Event Log on page 320
- Configuring an Accounting Policy on page 323
- Configuring Event Control on page 324
- Configuring a Log Filter on page 326
- Configuring an SNMP Trap Group on page 327
- Configuring a Syslog Target on page 328

Configuring an Event Log

A 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]
```

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 of compact flash (cf1:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See Configuring an Event Log on page 320 and Configuring a File ID on page 322.

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.

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:gal171>config>log# info
---------------------------------------------
        throttle-rate 500 interval 10
        event-control "aps" 2001 generate throttle
----------------------------------------------
*A:gal171>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 [regexp]
          severity {eq|neq|lt|lte|gt|gte} severity-level
          subject {eq|neq} subject [regexp]
```

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 cf1:
            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 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] [sn-
              mpv1|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|in-
           fo|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 330
- Deleting a Log File on page 332
- Modifying a File ID on page 333
- Deleting a File ID on page 335
- Modifying a Syslog ID on page 336
- Deleting a Syslog on page 337
- Modifying an SNMP Trap Group on page 338
- Deleting an SNMP Trap Group on page 339
- Modifying a Log Filter on page 340
- Deleting a Log Filter on page 342
- Modifying Event Control Parameters on page 343
- Returning to the Default Event Control Configuration on page 344

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 cf1:
             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 cf1:
            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 cf1:
            rollover 2880 retention 500
        exit
...
----------------------------------------------
```

```
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|in-
          fo|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 communityName |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 [regexp]
           severity {eq|neq|lt|lte|gt|gte} severity-level
           subject {eq|neq} subject [regexp]
```

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] gen-
        erate[severity-level] [throttle]
  event-control application-id [event-name|event-number] sup-
        press
```

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-nunmber]
```

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

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 Configuration Commands

```
config
    — log
            — event-control application-id [event-name | event-number] [generate [severity-level] [throttle]
            — 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]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 [regexp]
                         — no router
                         — severity {eq | neq | lt | lte | gt | gte} severity-level
                         — no severity
                         — subject {eq | neq} subject [regexp]
                         — 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 syslog-level
                    — 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** *string*
no description

Context config>log>filter
config>log>filte>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 *string* — 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** *log-id* — When a *log-id* 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 **event-control** *application-id* [*event-name* **|** *event-number*] [**generate** [*severity-level*] [**throttle**]
event-control *application-id* [*event-name* **|** *event-number*] **suppress**
no event-control *application* [*event-name* **|** *event-number*]

Context config>log

Description This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.

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.

Events are generated with a default severity level that can be modified by using the *severity-level* option.

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.

The rate of event generation can be throttled by using the **throttle** parameter.

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.

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 *application-id* — The application whose events are affected by this event control filter.

Default None, this parameter must be explicitly specified.

Values A valid application name. To display a list of valid application names, use the **applications** command. Valid applications are:

event-name | *event-number* — 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.

Default none

Values A valid event name or event number.

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 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.

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

Default no route-preference

Parameters **primary —** Specifies the primary routing preference for traffic generated for SNMP notifications and syslog messages.

Default outband

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.

Default inband

inband — Specifies that the logging utility will attempt to use the base routing context to send SNMP notifications and syslog messages to remote destinations.

outband — Specifies that the logging utility will attempt to use the management routing context to send SNMP notifications and syslog messages to remote destinations.

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** *file-id*

Context config>log

Description This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.

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.

A file ID can only be assigned to either *one* **log-id** or *one* **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.

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.

The file names for a log are created by the system as summarized in the table below:

File Type	File Name
Log File	`log`*`llff-timestamp`*
Accounting File	`act`*`aaff-timestamp`*

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***]**
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 medium severity trap is issued to indicate that a compact flash is either not available or that no space is available on the specified flash and that the backup location is being used.

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 becomes available, then the alarm condition will be cleared.

Use the **no** form of this command to revert to default settings.

NOTE: USB Flash is applicable only to platforms that support USB port and USB storage device (For example: 7210 SAS-E, 7210 SAS-K).

Default Log files are created on cf1: and accounting files are created on cf1:.

Parameters *cflash-id* — Specify the primary location.

Values cflash-id: **cf1:|uf1:**

usb-flash-id — Specifies the USB location.

rollover

Syntax **rollover** *minutes* [**retention** *hours*]
no rollover

Context config>log>file *file-id*

Description This command configures how often an event or accounting log is rolled over or partitioned into a new file.

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.

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.

When multiple **rollover** commands for a *file-id* are entered, the last command overwrites the previous command.

Default **rollover 1440 retention 12**

Parameters *minutes* — The rollover time, in minutes.

Values 5 — 10080

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** *filter-id*

Context config>log

Description 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.

Filters are configured in the **filter** *filter-id* context and then applied to a log in the **log-id** *log-id* context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.

Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.

The **no** form of the command removes the filter association from log IDs which causes those logs to forward all events.

Default No event filters are defined.

Parameters filter-id — The filter ID uniquely identifies the filter.

Values 1 — 1001

default-action

Syntax **default-action** {**drop** | **forward**}
no default-action

Context config>log>filter *filter-id*

Description 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.

When multiple **default-action** commands are entered, the last command overwrites the previous command.

The **no** form of the command reverts the default action to the default value (forward).

Default **default-action forward** — The events which are not explicitly dropped by an event filter match are forwarded.

Parameters **drop —** The events which are not explicitly forwarded by an event filter match are dropped.

forward — The events which are not explicitly dropped by an event filter match are forwarded.

Log Filter Entry Commands

action

Syntax **action** {**drop** | **forward**}
no action

Context config>log>filter *filter-id*>entry *entry-id*

Description 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.

Multiple action statements entered will overwrite previous actions.

The **no** form of the command removes the specified **action** statement.

Default Action specified by the **default-action** command will apply.

Parameters **drop —** Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

entry

Syntax [**no**] **entry** *entry-id*

Context config>log>filter *filter-id*

Description This command is used to create or edit an event filter entry. Multiple entries may be created using unique *entry-id* numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.

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.

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.

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.

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 *filter-id*>entry *entry-id*

Description 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.

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.

Use the **application** command to display a list of the valid applications.

Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Default No match context is defined.

application

Syntax **application** {**eq | neq**} *application-id*
no application

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an OS application as an event filter match criterion.

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.

The **no** form of the command removes the application as a match criterion.

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.

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**} *router-instance* [**regexp**]
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.

router-instance — Specifies a router name up to 32 characters to be used in the match criteria.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** 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**} *severity-level*
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** *syslog-id*

Context config>log

Description This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.

A valid *syslog-id* must have the target syslog host address configured.

A maximum of 10 syslog-id's can be configured.

No log events are sent to a syslog target address until the syslog-id has been configured as the log destination (**to**) in the log-id node.

Default No syslog IDs are defined.

Parameters *syslog-id* — The syslog ID number for the syslog destination, expressed as a decimal integer.

Values 1 — 10

address

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

Context config>log>syslog *syslog-id*

Description This command adds the syslog target host IP address to/from a syslog ID.

This parameter is mandatory. If no **address** is configured, syslog data cannot be forwarded to the syslog target host.

Only one address can be associated with a *syslog-id*. If multiple addresses are entered, the last address entered overwrites the previous address.

The same syslog target host can be used by multiple log IDs.

The **no** form of the command removes the syslog target host IP address.

Default **no address** — There is no syslog target host IP address defined for the syslog ID.

Parameters *ip-address* — The IP address of the syslog target host in dotted decimal notation.

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

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** *log-prefix-string*
no log-prefix

Context config>log>syslog *syslog-id*

Description This command adds the string prepended to every syslog message sent to the syslog host.

RFC3164, *The BSD syslog Protocol,* 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.

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.

The **no** form of the command removes the log prefix string.

Default **no log-prefix** — no prepend log prefix string defined.

Parameters *log-prefix-string* — An alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

level

Syntax **level** *syslog-level*
no level

Context config>log>syslog *syslog-id*

Description 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.

Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.

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** *events* [**interval** *seconds*]
no throttle-rate

Context config>log

Description This command configures an event throttling rate.

Parameters *events* — 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

interval *seconds* — 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** *log-id*

Context config>log

Description This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.

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.

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.

The **no** form of the command deletes the SNMP trap group.

Default There are no default SNMP trap groups.

Parameters *log-id* — 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 *log-id* exists.

Values 1 — 100

snmp-dying-gasp

Syntax **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*}]]
no snmp-dying-gasp

Context config>log

Description **Platforms Supported:** 7210 SAS-E, 7210 SAS-D, and 7210 SAS-K.

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:

1. Primary SNMP trap receiver.
2. Secondary SNMP trap receiver.
3. Tertiary SNMP trap receiver.

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 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.

Values 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** *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*

Context config>log>snmp-trap-group

Description 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.

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.

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:

- 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.

A single **snmp-trap-group** *log-id* can have multiple trap-receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.

Note that if the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* 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.

The **no** form of the command removes the SNMP trap receiver from the SNMP trap group.

Default No SNMP trap targets are defined.

Parameters *name* — 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:x (eight 16-bit pieces) x: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** *filter-id*
no filter

Context config>log>log-id *log-id*

Description This command adds an event filter policy with the log destination.

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.

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**.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the **filter** command.

Only one filter-id can be configured per log destination.

The **no** form of the command removes the specified event filter from the *log-id*.

Default **no filter** — No event filter policy is specified for a *log-id.*

Parameters *filter-id.* The event filter policy ID is used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in **config>log>filter** *filter-id*.

Values 1 — 1001

from

Syntax **from** {[**main**] [**security**] [**change**] [**debug-trace**]}
no from

Context config>log>log-id *log-id*

Description This command selects the source stream to be sent to a log destination.

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**).

Only one **from** command may be entered for a single *log-id*. If multiple **from** commands are configured, then the last command entered overwrites the previous **from** command.

The **no** form of the command removes all previously configured source streams.

Default No source stream is configured.

Parameters ***main*** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. 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.

security — Instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. 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.

change — Instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. 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.

debug-trace — Instructs all debug-trace messages in the debug stream to be sent to the destination configured in the **to** command for this destination *log-id*. Filters applied to debug messages are limited to application and subject.

log-id

Syntax [**no**] **log-id** *log-id*

Context config>log

Description This command creates a context to configure destinations for event streams.

The **log-id** context is used to direct events, alarms/traps, and debug information to respective destinations.

A maximum of 10 logs can be configured.

Before an event can be associated with this log-id, the **from** command identifying the source of the event must be configured.

Only one destination can be specified for a *log-id*. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.

Use the **event-control** command to suppress the generation of events, alarms, and traps for all log destinations.

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.

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.

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.

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** [*size*]

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 memory log. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.

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 none

Parameters *size* — The *size* parameter indicates the number of events that can be stored in the memory.

Default 100

Values 50 — 1024

to session

Syntax **to session**

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 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 *session* destination is not saved in the configuration 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 none

to snmp

Syntax **to snmp** [*size*]

Context config>log>log-id *log-id*

Description 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 *log-id*.

A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the *log-id*.

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 none

Parameters *size* — The *size* parameter defines the number of events stored in this memory log.

Default 100

Values 50 — 1024

to syslog

Syntax **to syslog** *syslog-id*

Context config>log>log-id

Description 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 a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1k bytes.

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 none

Parameters *syslog-id* — Instructs the events selected for the log ID to be directed to the *syslog-id*. The characteristics of the *syslog-id* referenced here must have been defined in the **config>log>syslog** *syslog-id* 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** *policy-id*
no accounting-policy *policy-id*

Context config>log

Description This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.

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.

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.

Network accounting policies are policies that can be applied to one or more network ports. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports where this policy is applied.

If no accounting policy is defined on a network port, 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.

In the 7210 SAS-E a total of 9 accounting records are available. In the 7210 SAS-D a total of 16 accounting records are available.

There are three types of accounting policies:

- Access
- Access port
- Network

When creating accounting policies, one access, one access port and one network 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.

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.

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 and one network 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.

Sample output for 7210 SAS-E:

```
A:7210-SASE>show>log# accounting-records

==========================================================
Accounting Policy Records
==========================================================
Record # Record Name                        Def. Interval
----------------------------------------------------------
1        service-ingress-octets             5
3        service-ingress-packets            5
4        service-egress-packets             5
5        network-ingress-octets             15
7        network-ingress-packets            15
8        network-egress-packets             15
32       saa                                5
36       access-egress-packets              5
41       combined-service-ing-egr-packets   5
42       combined-network-ing-egr-pkts      15
==========================================================
A:7210-SASE>show>log#
```

Sample output for 7210 SAS-D:

```
A:7210-SASD>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
32       saa                                5
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-SASD>show>log#
```

Sample output for 7210 SAS-K:

```
*A:7210SASk>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
32       saa                                5
58       combined-network-egress            15
59       combined-service-egress            5
===========================================================
*A:7210SASk>show>log#
```

To configure an accounting policy for access SAPs, select a service record (for example, service-ingress-octets).   To change the record name to another service record then the record command with the new record name can be entered and it will replace the old record name.

To configure an accounting policy for access ports, select access port type records such as access-egress packets. When changing the record name to another access port record, the record command with the new record name can be entered, and it will replace the old record name.

When configuring an accounting policy for network ports, a network record should be selected. When changing the record name to another network record, the record command with the new record name can be entered and it will replace the old record name.

If the change required modifies the record fromone 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-packets** 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.

to

Syntax **to file** *file-id*

Context config>log>accounting-policy *policy-id*

Description This command specifies the destination for the accounting records selected for the accounting policy.

Default No destination is specified.

Parameters *file-id* — The *file-id* 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.

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.

If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

Values 1 — 99

log-memory

Syntax **log-memory**
[no] log-memory

Context config>log>accounting-policy

Description 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.

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).

Default By default an accounting record is not configured to use temporary storage.

Parameters *Size* — 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 32KB of memory.

Show Commands

accounting-policy

Syntax **accounting-policy** [*acct-policy-id*] [**access** | **network**]

Context show>log

Description This command displays accounting policy information.

Parameters *policy-id* — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 — 99

access — Only displays access accounting policies.

network — Only displays network accounting policies.

Output **Accounting Policy Output —** The following table describes accounting policy output fields.

Table 43: Show Accounting Policy Output Fields

Label	Description
`Policy ID`	The identifying value assigned to a specific policy.
`Type`	Identifies accounting record type forwarded to the configured accounting file. `access` — Indicates that the policy is an access accounting policy. `network` — Indicates that the policy is a network accounting policy. `access port` — Indicates that the policy is an access port accounting policy which can be used to collect accounting records only for access ports. `none` — Indicates no accounting record types assigned.
`Def`	`Yes` — Indicates that the policy is a default access or network policy. `No` — Indicates that the policy is not a default access or network policy.
`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.

Table 43: Show Accounting Policy Output Fields (Continued)

Label	Description (Continued)
	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:

```
===============================
Accounting Policies
===============================================================================
Policy Type       Def Admin Oper  Intvl File Record Name
Id                    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
....
```

Sample Output

```
A:ALA-1# show log accounting-policy
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
==============================================================================
A:ALA-1#


A:ALA-1# show log accounting-policy 10
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 service-ingress-octets

Description : (Not Specified)

This policy is applied to:
    Svc Id: 100  SAP : 1/1/8:0     Collect-Stats
    Svc Id: 101  SAP : 1/1/8:1     Collect-Stats
    Svc Id: 102  SAP : 1/1/8:2     Collect-Stats
    Svc Id: 103  SAP : 1/1/8:3     Collect-Stats
    Svc Id: 104  SAP : 1/1/8:4     Collect-Stats
    Svc Id: 105  SAP : 1/1/8:5     Collect-Stats
    Svc Id: 106  SAP : 1/1/8:6     Collect-Stats
    Svc Id: 107  SAP : 1/1/8:7     Collect-Stats
    Svc Id: 108  SAP : 1/1/8:8     Collect-Stats
    Svc Id: 109  SAP : 1/1/8:9     Collect-Stats
...
==============================================================================
A:ALA-1#

A:ALA-1# show log accounting-policy network
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
==============================================================================
A:ALA-1#


A:ALA-1# show log accounting-policy access
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
```

```
Id                 State State           Id
------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 service-ingress-octets
==============================================================================
A:ALA-1#
```

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 44: 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-E)

```
A:7210-SASE>show>log# accounting-records

==========================================================
Accounting Policy Records
==========================================================
Record # Record Name                        Def. Interval
----------------------------------------------------------
1        service-ingress-octets             5
3        service-ingress-packets            5
4        service-egress-packets             5
5        network-ingress-octets             15
7        network-ingress-packets            15
8        network-egress-packets             15
32       saa                                5
36       access-egress-packets              5
41       combined-service-ing-egr-packets   5
42       combined-network-ing-egr-pkts      15
==========================================================
A:7210-SASE>show>log#
```

Sample Output (for 7210 SAS-D)

```
A:7210-SASD>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
32       saa                                5
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-SASD>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
SVCMGR
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.

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.

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.

Label	Description (Continued)
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

```
Sample output 7210 SAS-E:

*A:7210-SAS-E>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          4           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
   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          0           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
ETH_CFM:
   2001 dot1agCfmFaultAlarm              MI  gen       6297           0
   2002 tmnxDot1agCfmMepLbmTestComplete  MI  gen          0           0
   2003 tmnxDot1agCfmMepLtmTestComplete  MI  gen          0           0
   2004 tmnxDot1agCfmMepEthTestComplete  MI  gen          0           0
   2005 tmnxDot1agCfmMepDMTestComplete   MI  gen          0           0
   2006 tmnxDot1agCfmMepAisStateChanged  MI  gen         38           0
   2007 tmnxDot1agCfmMipEvaluation       MI  gen          0           0
ERING:
   2001 tmnxEthRingPathFwdStateChange    MI  gen       2911           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          2           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
LAG:
   2001 DynamicCostOn                    WA  gen          0           0
   2002 DynamicCostOff                   WA  gen          0           0
   2003 LagPortAddFailed                 WA  gen       1672           0
   2004 LagSubGroupSelected              WA  gen          0           0
   2005 LagPortAddFailureCleared         WA  gen       1672           0
LLDP:
   2001 lldpRemTablesChange              MI  gen       1298           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         18           0
   2010 tmnxClear                        IN  gen        750           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
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
NTP:
   2001 tmnxNtpAuthMismatch              WA  gen          0           0
   2002 tmnxNtpNoServersAvail            MA  gen          0           0
   2003 tmnxNtpServersAvail              MI  gen          0           0
   2008 tmnxNtpOperChange                WA  gen          1           0
   2009 tmnxNtpServerChange              MI  gen          1           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 tmnxOamLdpTtraceAutoDiscState    MI  gen          0           0
   2056 tmnxOamLdpTtraceFecProbeState    MI  gen          0           0
   2057 tmnxOamLdpTtraceFecDisStatus     MI  gen          0           0
   2101 tmnxOamSaaThreshold              MI  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         11           0
   2006 SFPRemoved                       MI  gen          0           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
   2017 etherAlarmSet                    MI  gen          0           0
   2018 etherAlarmClear                  MI  gen          0           0
   2019 ds1LoopbackStart                 MI  gen          0           0
   2020 ds1LoopbackStop                  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         19           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
SECURITY:
L  2001 cli_user_login                   MI  gen          6           0
L  2002 cli_user_logout                  MI  gen          3           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         1           0
L  2015 user_disconnect                  MA  gen         0           0
L  2016 radiusSystemIpAddrNotSet         MA  gen         0           0
   2018 tacplusOperStatusChange          MI  gen         2           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         1           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        28           0
   2207 tmnxConfigCreate                 WA  gen        11           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      6313           0
   2005 linkUp                           WA  gen      5315           0
   2101 risingAlarm                      MA  gen         2           0
   2102 fallingAlarm                     MA  gen         4           0
   2201 snmpdError                       MA  gen         0           0
STP:
   2001 topologyChangeSapMajorState      WA  gen      6756           0
   2002 newRootSap                       WA  gen         0           0
   2003 topologyChangeVcpState           WA  gen         0           0
   2004 newRootVcpState                  WA  gen         0           0
   2005 topologyChangeSapState           WA  gen       201           0
   2006 receivedTCN                      WA  gen         0           0
   2007 newRootBridge                    WA  gen      3138           0
   2008 unacknowledgedTCN                WA  gen         0           0
   2009 higherPriorityBridge             WA  gen         0           0
   2011 sapEncapPVST                     MI  gen         2           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       373           0
   2022 tmnxNewMstiRegionalRootBridge    WA  gen       6279           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
   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
SVCMGR:
   2011 svcTlsMacPinningViolation        WA  gen          0           0
   2103 svcStatusChanged                 MI  gen       1302           0
   2104 svcTlsFdbTableFullAlarmRaised    MI  gen          0           0
   2105 svcTlsFdbTableFullAlarmCleared   MI  gen          0           0
   2108 iesIfStatusChanged               MI  gen         10           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       2138           0
   2204 sapTlsMacAddrLimitAlarmRaised    MI  gen          2           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       3330           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 svcFdbMimDestTblFullAlrm         MI  gen          0           0
   2516 svcFdbMimDestTblFullAlrmCleared  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       9444           0
   2007 tmnxConfigCreate                 WA  gen       1340           0
   2008 tmnxConfigDelete                 WA  gen        401           0
   2009 tmnxStateChange                  WA  gen       1594           0
   2010 tmnxModuleMallocFailed           MA  gen          0           0
   2011 tmnxTrapDropped                  MA  gen          1           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           3
   2104 smScriptException                MI  sup          0           0
   2500 tmnxDyingGasp                    MI  gen          0           0
USER:
L  2001 cli_user_login                   MI  gen          6           0
L  2002 cli_user_logout                  MI  gen          3           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 cli_user_io                      MI  sup          0        4722
L  2010 snmp_user_set                    MI  sup          0        7881
L  2011 cli_config_io                    MI  gen        384           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:7210-SAS-E>show>log#
```

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.

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.
`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.

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 45: Event Log Filter Summary Output Fields

Label	Description
`Filter Id`	The event log filter ID.

Table 45: Event Log Filter Summary Output Fields (Continued)

Label	Description
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 46: 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 47: 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. `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** *router-instance* 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 matc

Table 47: Log Filter Match Criteria Output Fields (Continued)

Label	Description (Continued)
	`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
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 48: Show Log-Collector Output Fields

Label	Description
`<Collector Name>`	`Main` — The main event stream contains the events that are not explicitly directed to any other event stream.

Table 48: Show Log-Collector Output Fields (Continued)

Label	Description (Continued)
	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.
	Change — The change event stream contains all events that directly affect the configuration or operation of this node.
	Debug — The debug-trace stream contains all messages in the debug stream.
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	Enabled — Logging is enabled.
	Disabled — Logging is disabled.
Dest. Type	Console — A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether a user is logged in to the console or not. 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.
	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.

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** [*log-id*] [**severity** *severity-level*] [**application** *application*] [**sequence** *from-seq* [*to-seq*]] [**count** *count*] [**router** *router-instance* [**expression**]] [**subject** *subject* [**regexp**]] [**ascending | descending**]

Context show>log

Description This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.

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.

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.

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.

Parameters *log-id* — 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.

Default Displays the event log summary

Values 1 — 99

severity *severity-level* — Displays only events with the specified and higher severity.

Default All severity levels

Values cleared, indeterminate, critical, major, minor, warning

application *application* — Displays only events generated by the specified application.

Default All applications

expression — Specifies to use a regular expression as match criteria for the router instance string.

sequence *from-seq* [*to-seq*] — Displays the log entry numbers from a particular entry sequence number (*from-seq*) to another sequence number (*to-seq*). The *to-seq* value must be larger than the *from-seq* value.

If the *to-seq* 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**.

Default All sequence numbers

Values 1 — 4294967295

count *count* — Limits the number of log entries displayed to the *number* specified.

Default All log entries

Values 1 — 4294967295

router-instance — Specifies a router name up to 32 characters to be used in the display criteria.

subject *subject* — Displays only log entries matching the specified text *subject* 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.

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.

Label	Description (Continued)
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.
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 49: 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,

Table 49: SNMP Trap Group Output Fields (Continued)

Label	Description
`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 snmpv1, snmpv2c, snmpv3.
`Community`	The community string required by **snmpv1** or **snmpv2c** 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 50: 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.
`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** *log-id*

Context clear

Description 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.

This command is only applicable to event logs that are directed to file destinations and memory destinations.

SNMP, syslog and console/session logs are not affected by this command.

Parameters *log-id.* The event log ID to be initialized/rolled over.

Values 1 — 100

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

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 8 illustrates the relationship of log events, alarms and the LEDs.

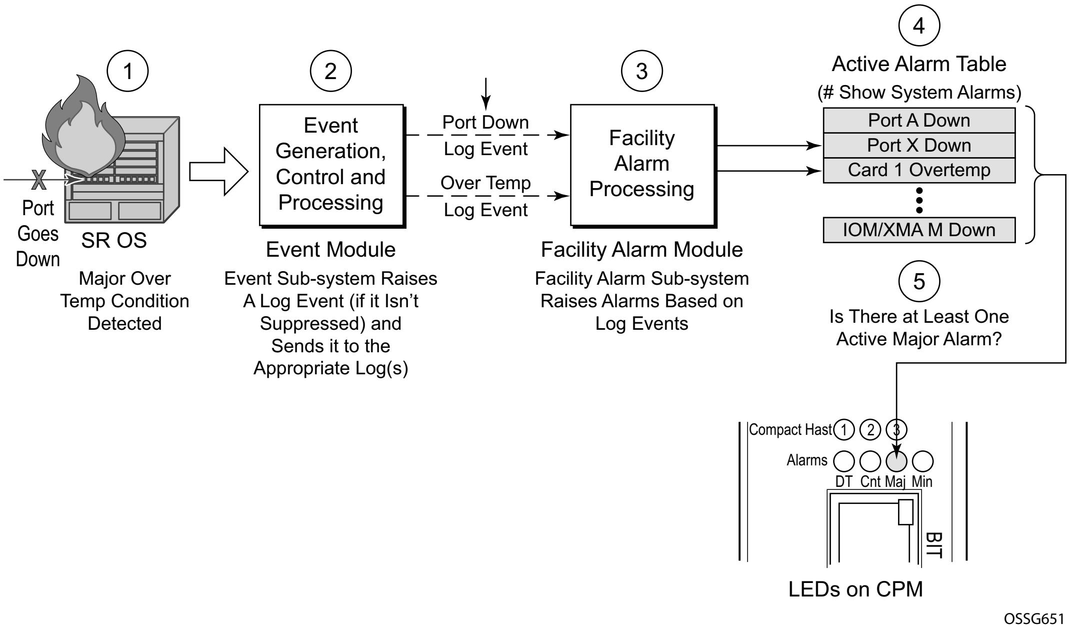

1
2
3
4
5
Port Goes Down
SR OS
Major Over Temp Condition Detected
Event Generation, Control and Processing
Event Module
Event Sub-system Raises A Log Event (if it Isn't Suppressed) and Sends it to the Appropriate Log(s)
Port Down Log Event
Over Temp Log Event
Facility Alarm Processing
Facility Alarm Module
Facility Alarm Sub-system Raises Alarms Based on Log Events
Active Alarm Table
(# Show System Alarms)
Port A Down
Port X Down
Card 1 Overtemp
IOM/XMA M Down
Is There at Least One Active Major Alarm?
Compact Hast
Alarms
DT Cnt Maj Min
BIT
LEDs on CPM
OSSG651

Figure 8: 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 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 51: 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			
				D	E	7210 SAS-K 2F2T1C	7210 SAS-K 2F2T1C
7-2001-1	tmnxEqCardFailure	Class MDA Module: failed, reason: MDA 1 failed startup tests	tmnxChassisNotificationClear	N	N	N	N
7-2003-1	tmnxEqCardRemoved	Class CPM Module: removed	tmnxEqCardInserted	N	N	N	N
7-2004-1	tmnxEqWrongCard	Class IOM Module: wrong type inserted	tmnxChassisNotificationClear	N	N	N	N
7-2005-1	tmnxEnvTempTooHigh	Chassis 1: temperature too high	tmnxChassisNotificationClear	Y	Y	Y	Y
7-2006-1	tmnxEqFanFailure	Fan 1 failed	tmnxChassisNotificationClear	N	Y	N	N
7-2007-1	tmnxEqPowerSupplyFailureOvt	Power supply 2 over temperature	tmnxChassisNotificationClear	N	N	N	N

Table 51: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event	7210 SAS Devices			
				D	E	7210 SAS-K 2F2T1 C	7210 SAS-K 2F2T1 C
7-2008-1	tmnxEqPowerSupplyFailureAc	Power supply 1 AC failure	tmnxChassisNotificationClear	N	N	Y (ETR)	N
7-2009-1	tmnxEqPowerSupplyFailureDc	Power supply 2 DC failure	tmnxChassisNotificationClear	Y (ETR)	N	N	N
7-2011-1	tmnxEqPowerSupplyRemoved	Power supply 1, power lost	tmnxEqPowerSupplyInserted	N (ETR and Non-ETR)	Y	N	N
7-2017-1	tmnxEqSyncIfTimingHoldover	Synchronous Timing interface in holdover state	tmnxEqSyncIfTimingHoldoverClear	Y	N	Y	Y
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Synchronous Timing interface, alarm los on reference 1	tmnxEqSyncIfTimingRef1AlarmClear	Y	N	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	N	Y	Y

Table 51: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event	7210 SAS Devices			
				D	E	7210 SAS-K 2F2T1C	7210 SAS-K 2F2T1C
7-2019-3	tmnxEqSyncIfTimingRef1 Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	Synchronous Timing interface, alarm oopir on reference 1	same as 7-2019-1	Y	N	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	N	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	N	N
7-2033-1	tmnxChassisUpgradeInProgress	Class CPM Module: software upgrade in progress	tmnxChassisUpgradeComplete	N	N	N	N
7-2050-1	tmnxEqPowerSupplyFailureInput	Power supply 1 input failure	tmnxChassisNotificationClear	Y (ETR)	N	N	N

Table 51: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event	7210 SAS Devices			
				D	E	7210 SAS-K 2F2T1 C	7210 SAS-K 2F2T1 C
7-2051-1	tmnxEqPowerSupplyFailureOutput	Power supply 1 output failure	tmnxChassisNotificationClear	N	Y	N	N
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	N	N
3-2004-1	linkDown	Interface intf-towards-node-B22 is not operational	linkUp	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 53: linkDown Facility Alarm Support

Object	Supported?
Ethernet Ports	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 430
- Common Configuration Tasks on page 431

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 431

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 433
- Show Commands on page 433

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** *max-alarms*

Context config>system>alarms

Description This command configures the maximum number of cleared alarms that the system will store and display.

Default 500

Parameters *max-alarms* — 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 `show system alarms` 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 54: 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#
```

```
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
===============================================================================
```

1 Standards and Protocol Support

Note: The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

Conventions followed:

- M(A,N) stands for 7210 SAS-M in both Access-uplink mode and Network mode. Similarly M(N) stands for 7210 SAS-M in network mode only.
- T(A,N) stands for 7210 SAS-M in both Access-uplink mode and Network mode. Similarly T(N) stands for 7210 SAS-T in network mode only.
- K5 stands for 7210 SAS-K 2F2T1C
- K12 stands for 7210 SAS-K 2F4T6C
- Sx stands for all variants of 7210 SAS-Sx-1/10GE.
- S stands for all variants of 7210 SAS-S-1/10GE platforms.
- Sx-1/10GE stands for only the variants of 7210 SAS-Sx-1/10GE
- R6 stands for 7210 SAS-R6
- R12 stands for 7210 SAS-R12
- D stands for 7210 SAS-D and 7210 SAS-D ETR, if a line item applies only to 7210 SAS-D ETR, then it is indicated as D-ETR.
- E means 7210 SAS-E.
- X means 7210 SAS-X.

BGP

draft-ietf-idr-add-paths-04, Advertisement of Multiple Paths in BGP (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-idr-best-external-03, Advertisement of the best external route in BGP (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-sidr-origin-validation-signaling-04, BGP Prefix Origin Validation State Extended Community (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1772, Application of the Border Gateway Protocol in the Internet (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1997, BGP Communities Attribute (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2439, BGP Route Flap Damping (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2858, Multiprotocol Extensions for BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2918, Route Refresh Capability for BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3107, Carrying Label Information in BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3392, Capabilities Advertisement with BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4271, A Border Gateway Protocol 4 (BGP-4) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4360, BGP Extended Communities Attribute (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4724, Graceful Restart Mechanism for BGP (Helper Mode) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4760, Multiprotocol Extensions for BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4893, BGP Support for Four-octet AS Number Space (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5004, Avoid BGP Best Path Transitions from One External to Another (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5291, Outbound Route Filtering Capability for BGP-4 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5668, 4-Octet AS Specific BGP Extended Community (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6811, Prefix Origin Validation (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

Circuit Emulation

RFC 4553, Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP) (M(N))

RFC 5086, Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN) (M(N))

RFC 5287, Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks (M(N))

Ethernet

IEEE 802.1AB, Station and Media Access Control Connectivity Discovery (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1ad, Provider Bridges (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1ag, Connectivity Fault Management (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1ah, Provider Backbone Bridges (M(N), X, T(N))

IEEE 802.1ax, Link Aggregation (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1D, MAC Bridges (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1p, Traffic Class Expediting (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1Q, Virtual LANs (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1s, Multiple Spanning Trees (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1w, Rapid Reconfiguration of Spanning Tree (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.1X, Port Based Network Access Control (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ab, 1000BASE-T (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ac, VLAN Tag (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ad, Link Aggregation (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ae, 10 Gb/s Ethernet (M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ah, Ethernet in the First Mile (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3ba, 40 Gb/s and 100 Gb/s Ethernet (R6, R12)

IEEE 802.3i, Ethernet (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3u, Fast Ethernet (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 802.3z, Gigabit Ethernet (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.8032, Ethernet Ring Protection Switching (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, Operational management of Loop Free Alternates (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

IP — General

draft-grant-tacacs-02, The TACACS+ Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 768, User Datagram Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 793, Transmission Control Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 854, TELNET Protocol Specifications (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 951, Bootstrap Protocol (BOOTP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1034, Domain Names - Concepts and Facilities (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1035, Domain Names - Implementation and Specification (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1350, The TFTP Protocol (revision 2) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1534, Interoperation between DHCP and BOOTP (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1542, Clarifications and Extensions for the Bootstrap Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2131, Dynamic Host Configuration Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2347, TFTP Option Extension (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2348, TFTP Blocksize Option (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2349, TFTP Timeout Interval and Transfer Size Options (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2428, FTP Extensions for IPv6 and NATs (D, E, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2865, Remote Authentication Dial In User Service (RADIUS) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2866, RADIUS Accounting (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3046, DHCP Relay Agent Information Option (Option 82) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3596, DNS Extensions to Support IP version 6 (D, E, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3768, Virtual Router Redundancy Protocol (VRRP) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4251, The Secure Shell (SSH) Protocol Architecture (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4254, The Secure Shell (SSH) Connection Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5880, Bidirectional Forwarding Detection (BFD) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5881, Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5883, Bidirectional Forwarding Detection (BFD) for Multihop Paths (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6528, Defending against Sequence Number Attacks (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IP — Multicast

RFC 1112, Host Extensions for IP Multicasting (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2236, Internet Group Management Protocol, Version 2 (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3376, Internet Group Management Protocol, Version 3 (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3446, Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4604, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4607, Source-Specific Multicast for IP (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4608, Source-Specific Protocol Independent Multicast in 232/8 (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5059, Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5384, The Protocol Independent Multicast (PIM) Join Attribute Format (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6513, Multicast in MPLS/BGP IP VPNs (T(N), Mxp, Sx/S-1/10GE, R6, R12)

RFC 6514, BGP Encodings and Procedures for Multicast in MPLS/IP VPNs (T(N), Mxp, Sx/S-1/10GE, R6, R12)

RFC 6515, IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs (T(N), Mxp, Sx/S-1/10GE, R6, R12)

RFC 6625, Wildcards in Multicast VPN Auto-Discover Routes (T(N), Mxp, Sx/S-1/10GE, R6, R12)

RFC 6826, Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path (T(N), Mxp, Sx/S-1/10GE, R6, R12)

RFC 7385, IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points (T(N), Mxp, Sx/S-1/10GE, R6, R12)

IP — Version 4

RFC 791, Internet Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 792, Internet Control Message Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 826, An Ethernet Address Resolution Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1812, Requirements for IPv4 Routers (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1981, Path MTU Discovery for IP version 6 (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2401, Security Architecture for Internet Protocol (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

IP — Version 6

RFC 2464, Transmission of IPv6 Packets over Ethernet Networks (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3021, Using 31-Bit Prefixes on IPv4 Point-to-Point Links (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3587, IPv6 Global Unicast Address Format (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4007, IPv6 Scoped Address Architecture (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4193, Unique Local IPv6 Unicast Addresses (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4291, Internet Protocol Version 6 (IPv6) Addressing Architecture (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4861, Neighbor Discovery for IP version 6 (IPv6) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4862, IPv6 Stateless Address Autoconfiguration (Router Only) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5095, Deprecation of Type 0 Routing Headers in IPv6 (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5952, A Recommendation for IPv6 Address Text Representation (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6106, IPv6 Router Advertisement Options for DNS Configuration (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6164, Using 127-Bit IPv6 Prefixes on Inter-Router Links (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

IPsec

RFC 2401, Security Architecture for the Internet Protocol (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2406, IP Encapsulating Security Payload (ESP) (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

IS-IS

draft-ietf-isis-mi-02, IS-IS Multi-Instance (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-kaplan-isis-ext-eth-02, Extended Ethernet Frame Size Support (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

ISO/IEC 10589:2002, Second Edition, Nov. 2002, Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3359, Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3719, Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3787, Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4971, Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5120, M-ISIS: Multi Topology (MT) Routing in IS-IS (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5301, Dynamic Hostname Exchange Mechanism for IS-IS (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5302, Domain-wide Prefix Distribution with Two-Level IS-IS (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5303, Three-Way Handshake for IS-IS Point-to-Point Adjacencies (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5304, IS-IS Cryptographic Authentication (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5305, IS-IS Extensions for Traffic Engineering TE (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5306, Restart Signaling for IS-IS (Helper Mode) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5308, Routing IPv6 with IS-IS (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5310, IS-IS Generic Cryptographic Authentication (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6232, Purge Originator Identification TLV for IS-IS (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6233, IS-IS Registry Extension for Purges (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

Management

draft-ieft-snmpv3-update-mib-05, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-idr-bgp4-mib-05, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-isis-wg-mib-06, Management Information Base for Intermediate System to Intermediate System (IS-IS) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-mpls-ldp-mib-07, Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12) draft-ietf-mpls-lsr-mib-06, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-mpls-te-mib-04, Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-ietf-ospf-mib-update-08, OSPF Version 2 Management Information Base (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

ianaaddressfamilynumbers-mib, IANA-ADDRESS-FAMILY-NUMBERS-MIB (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

ianaiftype-mib, IANAifType-MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ianaiprouteprotocol-mib, IANA-RTPROTO-MIB (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE8021-CFM-MIB, IEEE P802.1ag(TM) CFM MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE8021-PAE-MIB, IEEE 802.1X MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE8023-LAG-MIB, IEEE 802.3ad MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

LLDP-MIB, IEEE P802.1AB(TM) LLDP MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1157, A Simple Network Management Protocol (SNMP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1215, A Convention for Defining Traps for use with the SNMP (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1724, RIP Version 2 MIB Extension (Mxp)

RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2115, Management Information Base for Frame Relay DTEs Using SMIv2 (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2138, Remote Authentication Dial In User Service (RADIUS) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2206, RSVP Management Information Base using SMIv2 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2213, Integrated Services Management Information Base using SMIv2 (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2494, Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type (M(N))

RFC 2571, An Architecture for Describing SNMP Management Frameworks (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2573, SNMP Applications (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2578, Structure of Management Information Version 2 (SMIv2) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2579, Textual Conventions for SMIv2 (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2819, Remote Network Monitoring Management Information Base (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2856, Textual Conventions for Additional High Capacity Data Types (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2863, The Interfaces Group MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2864, The Inverted Stack Table Extension to the Interfaces Group MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2933, Internet Group Management Protocol MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3014, Notification Log MIB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3164, The BSD syslog Protocol (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3165, Definitions of Managed Objects for the Delegation of Management Scripts (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3231, Definitions of Managed Objects for Scheduling Management Operations (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3273, Remote Network Monitoring Management Information Base for High Capacity Networks (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3419, Textual Conventions for Transport Addresses (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3593, Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals (K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3635, Definitions of Managed Objects for the Ethernet-like Interface Types (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3877, Alarm Management Information Base (MIB) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3895, Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types (M(N))

RFC 4001, Textual Conventions for Internet Network Addresses (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4022, Management Information Base for the Transmission Control Protocol (TCP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4113, Management Information Base for the User Datagram Protocol (UDP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4220, Traffic Engineering Link Management Information Base (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4292, IP Forwarding Table MIB (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4293, Management Information Base for the Internet Protocol (IP) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6241, Network Configuration Protocol (NETCONF) (K5, K12, R6, R12)

RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH) (K5, K12, R6, R12)

MPLS — General

RFC 3031, Multiprotocol Label Switching Architecture (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3032, MPLS Label Stack Encoding (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3443, Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4182, Removing a Restriction on the use of MPLS Explicit NULL (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5332, MPLS Multicast Encapsulations (T(N), Mxp, Sx/S-1/10GE, R6, R12)

MPLS — GMPLS

draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

MPLS — LDP

draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-pdutta-mpls-ldp-v2-00, LDP Version 2 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3037, LDP Applicability (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (Helper Mode) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5036, LDP Specification (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5443, LDP IGP Synchronization (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5561, LDP Capabilities (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6826, Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

MPLS — MPLS-TP

RFC 5586, MPLS Generic Associated Channel (T(N), R6, R12)

RFC 5921, A Framework for MPLS in Transport Networks (T(N), R6, R12)

RFC 5960, MPLS Transport Profile Data Plane Architecture (T(N), R6, R12)

RFC 6370, MPLS Transport Profile (MPLS-TP) Identifiers (T(N), R6, R12)

RFC 6378, MPLS Transport Profile (MPLS-TP) Linear Protection (T(N), R6, R12)

RFC 6426, MPLS On-Demand Connectivity and Route Tracing (T(N), R6, R12)

RFC 6428, Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile (T(N), R6, R12)

RFC 6478, Pseudowire Status for Static Pseudowires (T(N), R6, R12)

RFC 7213, MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing (T(N), R6, R12)

MPLS — OAM

RFC 6424, Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6425, Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping (T(N), Mxp, R6, R12)

MPLS — RSVP-TE

RFC 2702, Requirements for Traffic Engineering over MPLS (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2747, RSVP Cryptographic Authentication (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2961, RSVP Refresh Overhead Reduction Extensions (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3097, RSVP Cryptographic Authentication -- Updated Message Type Value (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) (M(N), T(N), X, Mxp, R6, R12)

RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4561, Definition of a Record Route Object (RRO) Node-Id Sub-Object (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4875, Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) (T(N), Mxp, R6, R12)

RFC 4950, ICMP Extensions for Multiprotocol Label Switching (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5712, MPLS Traffic Engineering Soft Preemption (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5817, Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

OSPF

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 1765, OSPF Database Overflow (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2328, OSPF Version 2 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3509, Alternative Implementations of OSPF Area Border Routers (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3623, Graceful OSPF Restart Graceful OSPF Restart (Helper Mode) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2 (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4222, Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4552, Authentication/Confidentiality for OSPFv3 (M(N), T(N), X, Mxp, R6, R12)

RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4970, Extensions to OSPF for Advertising Optional Router Capabilities (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5185, OSPF Multi-Area Adjacency (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5187, OSPFv3 Graceful Restart (Helper Mode) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5243, OSPF Database Exchange Summary List Optimization (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5250, The OSPF Opaque LSA Option (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5340, OSPF for IPv6 (M(N), T(N), X, Mxp, R6, R12)

RFC 5709, OSPFv2 HMAC-SHA Cryptographic Authentication (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5838, Support of Address Families in OSPFv3 (M(N), T(N), X, Mxp, R6, R12)

RFC 6987, OSPF Stub Router Advertisement (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, OAM Procedures for VPWS Interworking (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3916, Requirements for Pseudo- Wire Emulation Edge-to-Edge (PWE3) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4385, Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4446, IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5659, An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6073, Segmented Pseudowire (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6310, Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network (Mxp, R6, R12)

RFC 6718, Pseudowire Redundancy (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6870, Pseudowire Preferential Forwarding Status bit (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 7023, MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 7267, Dynamic Placement of Multi-Segment Pseudowires (M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

Quality of Service

RFC 2430, A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 2598, An Expedited Forwarding PHB (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3140, Per Hop Behavior Identification Codes (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 3260, New Terminology and Clarifications for Diffserv (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

RIP

RFC 1058, Routing Information Protocol (Mxp)

RFC 2082, RIP-2 MD5 Authentication (Mxp)

RFC 2453, RIP Version 2 (Mxp)

Timing

GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx-1/10GE, R6, R12)

ITU-T G.781, Synchronization layer functions, issued 09/2008 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.8261, Timing and synchronization aspects in packet networks, issued 04/2008 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.8262, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.8264, Distribution of timing information through packet networks, issued 10/2008 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

ITU-T G.8265.1, Precision time protocol telecom profile for frequency synchronization, issued 10/2010 (D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx-1/10GE, R6, R12)

ITU-T G.8275.1, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014 (R6, R12)

RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification (D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, R12)

VPLS

RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 5501, Requirements for Multicast Support in Virtual Private LAN Services (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs) (K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, R6, R12)

INDEX

Customer Document and Product Support

Customer documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation feedback

Customer Documentation Feedback