7210 Service Access System

Release 23.3.R1

7210 SAS-Mxp, R6, R12, S, Sx, T System Management Guide

3HE 19295 AAAA TQZZA
Edition 01
March 2023

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

List of tables

List of figures

1 Getting started

This chapter provides process flow information to configure system security and access functions, event and accounting logs. It also provides an overview of the document organization, content, and terminology used in this guide.

1.1 About this guide

Note:
Unless explicitly noted otherwise, this guide uses 7210 SAS-Dxp to refer to the 7210 SAS-Dxp 12p, 7210 SAS-Dxp 16p, and 7210 SAS-Dxp 24p platforms.

This guide describes router security, SNMP features, and event and accounting logs for the following 7210 SAS platforms, operating in one of the modes described in Table 1: Supported modes of operation and configuration methods. If multiple modes of operation apply, they are explicitly noted in the topic.

- 7210 SAS-Mxp
- 7210 SAS-R6
- 7210 SAS-R12
- 7210 SAS-Sx/S 1/10GE
- 7210 SAS-Sx 10/100GE
- 7210 SAS-T

See 7210 SAS modes of operation for information about the modes of operation supported by the 7210 SAS product family.

Note:
Unless explicitly noted otherwise, the phrase "Supported on all 7210 SAS platforms as described in this document" is used to indicate that the topic and CLI commands apply to all the 7210 SAS platforms in the following list, when operating in the specified modes only.

- network mode of operation

  7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, 7210 SAS-Sx 10/100GE, and 7210 SAS-T

- standalone mode of operation

  7210 SAS-Mxp, 7210 SAS-Sx/S 1/10GE, 7210 SAS-Sx 10/100GE

- standalone-VC mode of operation

  7210 SAS-Sx/S 1/10GE

If the topic and CLI commands are supported on the 7210 SAS-T operating in the access-uplink mode, it is explicitly indicated, where applicable.

1.1.1 Document structure and content

This guide uses the following structure to describe router security, SNMP features, and event and accounting log content.

Note:
This guide generically covers Release 23.*x*.R*x* content and may include some content that will be released in later maintenance loads. See the *7210 SAS Software Release Notes 23.x.Rx*, part number 3HE 19296 000*x* TQZZA, for information about features supported in each load of the Release 23.*x*.R*x* software.

- This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow. Each chapter describes a software area and provides CLI syntax and command usage to configure parameters for the functional area.
- Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.
- See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for boot options to configure the satellite mode of operation on the router. See the 7750 SR software user guides for information about service and protocol provisioning, and operating the 7210 SAS router in satellite mode.
- Unless explicitly noted, the CLI commands and their configuration is similar for both network and access-uplink operating modes for features applicable to both modes of operation.

1.2 7210 SAS modes of operation

Unless explicitly noted, the phrase "mode of operation" and "operating mode" refers to the current operating mode of the 7210 SAS router. Each operating mode provides configuration access to a specific group of CLI commands.

Note:
Not all CLI commands are supported on all 7210 SAS platforms in all modes of operation. Users can only configure CLI commands supported by the current operating mode of the router. See the *7210 SAS Software Release Notes 23.x.Rx*, part number 3HE 19296 000*x* TQZZA, and to the appropriate 7210 SAS software user guide for information about features and capabilities supported by a 7210 SAS platform when operating in a specific mode.

The following modes of operation are supported by the 7210 SAS product family.

- **access-uplink**

  In the access-uplink operating mode, the 7210 SAS router uplinks to the network using Layer 2 Ethernet VLAN switching (without IP/MPLS).

  Platforms Supported: 7210 SAS-D, 7210 SAS-Dxp, 7210 SAS-K 2F1C2T, 7210 SAS-K 2F6C4T, 7210 SAS-K 3SFP+ 8C, and 7210 SAS-T

- **network**

  In the network operating mode, the 7210 SAS router uses IP/MPLS uplinks to the network. The IP routing protocols and MPLS functionality is available; see the appropriate 7210 SAS software user guide for more information about supported features.

Platforms Supported: 7210 SAS-K 2F6C4T, 7210 SAS-K 3SFP+ 8C, 7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, 7210 SAS-Sx 10/100GE, and 7210 SAS-T

- **satellite**

  In the satellite operating mode, the 7210 SAS platform uses high-capacity uplinks (for example, 10GE ports on the 7210 SAS-Mxp and 100GE ports on the 7210 SAS-Sx 10/100GE) to connect to the 7750 SR host. The 7210 SAS router is managed by the 7750 SR host. There is no direct CLI access to the satellite node, and all services and protocols are configured on the host.

  Platforms Supported: 7210 SAS-Mxp, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-Sx 10/100GE

- **standalone**

  In the standalone operating mode, the 7210 SAS platform supports IP/MPLS uplinks. It is operated and managed independently.

  The functionality and features available on the standalone 7210 SAS platform are similar to the network operating mode. The standalone mode is primarily used to differentiate between a node being managed by the 7750 SR host (in the satellite operating mode), and a node managed independently (standalone operating mode).

  Platforms Supported: 7210 SAS-Mxp, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-Sx 10/100GE

- **standalone-VC**

  In the standalone-VC operating mode, a set of 7210 SAS devices are stacked to provide larger 1GE/10GE port density and control-plane redundancy. The stack of nodes is provisioned and managed as a single chassis, and not as individual nodes.

  The functionality and features available on the 7210 SAS platform are similar to the network operating mode, with additional capabilities, such as control-plane redundancy with non-stop routing and non-stop services.

  Platforms Supported: 7210 SAS-Sx/S 1/10GE

For 7210 SAS platforms that support multiple explicit modes of operation (Table 1: Supported modes of operation and configuration methods), the operating mode must be configured in the Boot Option File (BOF) to ensure the router boots up in the specified mode. For example, the 7210 SAS-T supports access-uplink and network modes of operation, and the 7210 SAS-Sx/S 1/10GE supports satellite, standalone, and standalone-VC mode of operations. In some cases, the 7210 SAS router operates in a specific mode implicitly, and explicit configuration is not required.

See the appropriate *Basic System Configuration Guide* for boot options and information about how to boot the 7210 SAS platform in a specific operating mode.

The following table lists the supported modes of operation and the configuration methods for the 7210 SAS platforms. Unless explicitly noted otherwise, the operating mode is supported on all variants of the specific 7210 SAS platform.

Table 1: Supported modes of operation and configuration methods

7210 SAS platform	Mode of operation and configuration method				
	Network	Access-uplink	Standalone	Standalone-VC	Satellite
7210 SAS-D		Implicit	Implicit		
7210 SAS-Dxp		Implicit	Implicit		

7210 SAS platform	Mode of operation and configuration method				
	Network	Access-uplink	Standalone	Standalone-VC	Satellite
7210 SAS-K 2F1C2T		Implicit	Implicit		
7210 SAS-K 2F6C4T [2]	Port Mode Configuration [1]	Port Mode Configuration [1]	Implicit		
7210 SAS-K 3SFP+ 8C [2]	Port Mode Configuration [1]	Port Mode Configuration [1]	Implicit		
7210 SAS-Mxp	Implicit [3]		Explicit BOF Configuration		Explicit BOF Configuration
7210 SAS-R6 [2]	Implicit		Implicit		
7210 SAS-R12 [2]	Implicit		Implicit		
7210 SAS-Sx/S 1/10GE	Implicit [3]		Explicit BOF Configuration	Explicit BOF Configuration	Explicit BOF Configuration
7210 SAS-Sx 10/100GE	Implicit [3]		Explicit BOF Configuration		Explicit BOF Configuration
7210 SAS-T	Explicit BOF Configuration	Explicit BOF Configuration	Implicit		

1.3 7210 SAS port modes

Unless explicitly noted, the phrase "port mode" refers to the current port configuration of the 7210 SAS node. The 7210 SAS platform supports the configuration of the following port modes.

- **access port mode**

  Access ports are configured for customer-facing traffic if Service Access Points (SAPs) are required. The appropriate encapsulation type must be configured to distinguish the services on the port; services are configured on the port based on the encapsulation value.

  Access ports can be configured on all the 7210 SAS platforms.

- **access-uplink port mode**

1 See 7210 SAS port modes for information about port mode configuration

2 By default, the 7210 SAS-K 2F6C4T and 7210 SAS-K 3SFP+ 8C boot up in the network mode of operation. These platforms also allow the use of access-uplink port mode (without explicit BOF configuration), which provides the option to use Layer 2 uplinks instead of IP/MPLS uplinks to the network core, similar to the 7210 SAS-K 2F1C2T router.

3 Implicitly operates in network mode when standalone mode of operation is configured

4 Supports MPLS uplinks only and implicitly operates in network mode

Access-uplink ports provide native Ethernet connectivity in service provider transport or in an infrastructure network. With this option, the encap-type can be configured to only QinQ. Access-uplink SAPs, which are QinQ SAPs, can only be configured on an access-uplink port to allow the operator to differentiate multiple services being carried over a single uplink port.

This is the default port mode of a 7210 SAS node in the access-uplink mode of operation.

- **network port mode**

  Network ports are configured for network-facing traffic in the service provider transport or infrastructure network, and provide IP/MPLS uplinks.

  This is the default port mode of a 7210 SAS node in the network or standalone mode of operation.

- **hybrid port mode**

  Hybrid ports are configured for access and network facing traffic, and allow a single port to operate in both access and network modes.

Port modes available for configuration on a 7210 SAS node are determined by the current mode of operation of the router.

Note:
The 7210 SAS-K 2F6C4T and 7210 SAS-K 3SFP+ 8C are unique; all port modes listed in Table 2: Supported port modes by mode of operation are available for configuration on the router, regardless of the current mode of operation.

The following table lists the port mode configuration support per 7210 SAS mode of operation.

Table 2: Supported port modes by mode of operation

Mode of operation	Supported port mode			
	Access	Network	Hybrid	Access-uplink
Access-uplink	✓			✓
Network	✓	✓	✓	
Satellite [5]				
Standalone	✓	✓	✓	
Standalone-VC	✓	✓	✓	

The following table lists the port mode configuration supported by the 7210 SAS product family. See the appropriate *Interface Configuration Guide* for more information about configuring the port modes for a specific platform.

[5] Port modes are configured on the 7750 SR host and managed by the host.

Table 3: 7210 SAS platforms supporting port modes

Platform	Port mode			
	Access	Network	Hybrid	Access-uplink
7210 SAS-D	Yes	No	No	Yes
7210 SAS-Dxp	Yes	No	No	Yes
7210 SAS-K 2F1C2T	Yes	No	No	Yes
7210 SAS-K 2F6C4T	Yes	Yes	Yes	Yes
7210 SAS-K 3SFP+ 8C	Yes	Yes	Yes	Yes
7210 SAS-Mxp	Yes	Yes	Yes	No
7210 SAS-R6 IMM-b (IMMv2)	Yes	Yes	Yes	No
7210 SAS-R6 IMM-c 100GE (IMM-c 1QSFP28)	Yes	Yes	Yes	No
7210 SAS-R12 IMM-b	Yes	Yes	Yes	No
7210 SAS-R12 IMM-c 100GE (IMM-c 1QSFP28)	Yes	Yes	Yes	No
7210 SAS-Sx/S 1/10GE	Yes	Yes	Yes	No
7210 SAS-Sx 10/100GE	Yes	Yes	Yes	No
7210 SAS-T	Yes	Yes [6]	Yes [7]	Yes [8]

1.4 7210 SAS system management configuration process

The following table 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.

6 Network ports are supported only if the node is operating in network mode.

7 Hybrid ports are supported only if the node is operating in network mode.

8 Access-uplink ports are supported only if the node is operating in access-uplink mode.

Table 4: Configuration process

Area	Task	Chapter
System security	Configure system security parameters, such as authentication, authorization, and accounting	Security
Network management	Configure SNMP elements	SNMP
Secure network management	Configure NETCONF elements	NETCONF
Operational functions	Configure event and accounting logs	Event and accounting logs
Facility alarms	Configure facility alarms	Facility alarms
Reference	List of IEEE, IETF, and other proprietary entities	Standards and protocol support

1.5 Conventions

This section describes the general conventions used in this guide.

1.5.1 Precautionary and information messages

The following information symbols are used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.5.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step:
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action:
   a. This is one substep.
   b. This is another substep.

2 Security

This chapter provides information to configure security parameters.

2.1 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 username 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.

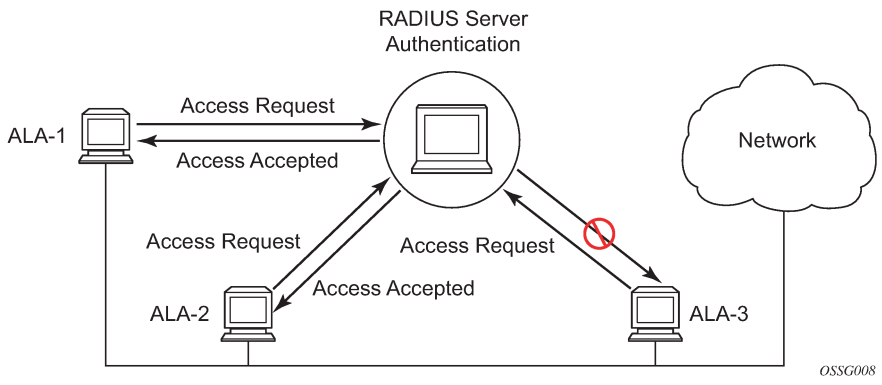
You can configure 7210 SAS routers to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, or FTP. You can select the authentication order which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

The 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.

The following figure shows how end user access-requests are sent to a RADIUS server. After validating the usernames and passwords, the RADIUS server returns an access-accept message to the users on ALA-1 and ALA-2. The username and password from ALA-3 could not be authenticated, therefore access was denied.

Figure 1: RADIUS requests and responses



2.1.1 Authentication

Authentication validates a username 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 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 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. Nokia recommends that the same user databases be maintained for RADIUS servers 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 the following authentication methods can be configured to control network access from a 7210 SAS-Series router.

2.1.1.1 Local authentication

Local authentication uses usernames and passwords to authenticate login attempts. The usernames 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 usernames and password management information. This is referred to as local authentication. Remote security servers such as RADIUS or TACACS+, are not enabled.

2.1.1.2 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.

2.1.1.2.1 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.

2.1.1.2.1.1 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.

2.1.1.2.1.2 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.

2.1.1.2.1.3 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 toward the RADIUS server is broken (for example, the route is not available, the is interface shutdown, and so on), 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, therefore, it is not certain yet whether the server is actually reachable).

2.1.1.2.1.4 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 username. 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).

  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).

2.1.1.3 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 specific 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.

2.1.1.4 Password hashing

The 7210 SAS supports two algorithms for user password hashing: bcrypt, which is the default algorithm, and PBKDF2. The PBKDF2 algorithm can use SHA2 (SHA-256) for hashing.

The password hashing algorithm can be configured using the **configure system security password hashing** command. The configured algorithm hashes all user passwords.

When password hashing is configured, the following sequence of steps occurs at login:

1. The node checks the stored password and notes its hash algorithm.
2. The password entered by the user is hashed with the noted algorithm, and the node compares the hash with the stored user password hash.
3. If the entered and stored passwords are the same, and if the hash algorithm of the stored user password is different than the hash algorithm of the system password, the user is prompted to enter a new password two times to ensure password match. The node stores this new password in the RAM (not in the system configuration file).

   To store the new password in the configuration file, an admin user must perform the **admin save** command. If the **admin save** command is not executed, on the next reboot the hash algorithm of the stored user password may be different than the system hash, and the user must go through this process again from step 2.

After an upgrade to a software load that supports PBKDF2, the default password continues to be stored using the bcrypt algorithm. The following example describes the procedure to change the algorithm. In this example, the algorithm is changed to PBKDF2, and "User_name" can be any user.

1. User_name logs in and runs the **hashing** command to change the algorithm.
2. To save the algorithm change, an admin user performs an **admin save** command.
3. To store User_name's password using PBKDF2, the admin user changes User_name's password.
4. From this point onward, any new user passwords or changes to existing user passwords are stored using PBKDF2.

2.1.2 Authorization

The OS support local, RADIUS, and TACACS+ authorization to control the actions of specific users by applying a profile based on username and password configurations when network access is granted. The profiles are configured locally as well as VSAs on the RADIUS server. See Vendor-specific attributes (VSAs).

When 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 5: Supported authorization configurations describes 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 5: Supported authorization configurations

User type	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. Usernames can be configured on the RADIUS server. Usernames 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.

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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.

2.1.3 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.

2.1.3.1 RADIUS accounting

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

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

2.1.3.2 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.

2.2 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. That is, 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.

The following table lists the types of security supported by each protocol.

Table 6: Security methods capabilities

Method	Authentication	Authorization	Accounting [9]
Local	Y	Y	N
TACACS+	Y	Y	Y
RADIUS	Y	Y	Y

2.2.1 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 whether 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 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 the Nokia 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.

2.2.2 Access request flow

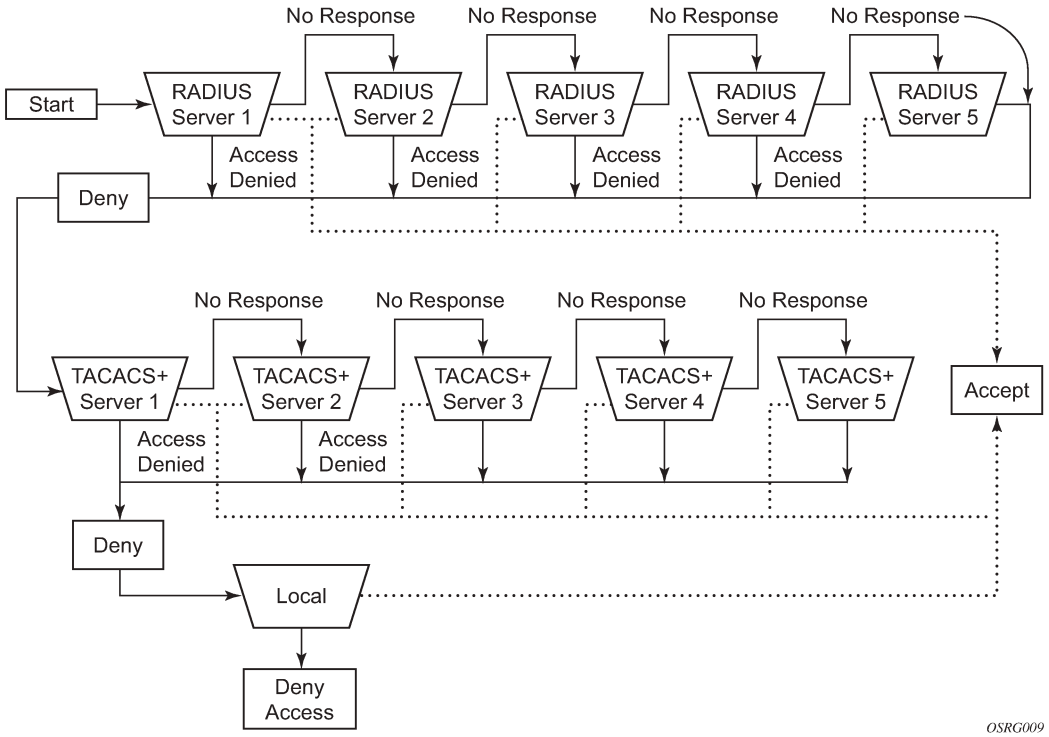
In Figure 2: Security flow, the authentication process is defined in the **config>system>security> password** context. The authentication order is determined by specifying the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords. This example uses the authentication 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

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

+ 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 username 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 username and password verification. This is the last chance for the access request to be accepted.

Figure 2: Security flow



2.3 Control and management traffic protection

7210 SAS platforms support an extensive set of configurable mechanisms to protect the CPU from being flooded with control or management traffic.

These protection mechanisms are a set of configurable hardware-based filters, classification, queuing, and rate-limiting functions that drop unwanted traffic before it reaches the control processor:

- In-band traffic extracted from line cards to the control processing module (CPM) on chassis-based systems, or extracted from front-panel ports on fixed form-factor devices:
  - Line card or fixed form-factor platform features:
    - ACLs filters: IPv4, IPv6, and MAC
    - Distributed CPU protection (supported only on the 7210 SAS-R6 and 7210 SAS-R12)
  - CPM features:

    - Centralized CPU protection
- Out-band and in-band traffic: management access filters

2.3.1 CPM Management Access Filters

CPM traffic is extracted from the data plane and sent to the CPM for processing. Packets from all network and access ports can be filtered using management access filters, which use CPU resources. Packets originating from a management Ethernet port can also be filtered using management access filters.

2.3.1.1 CPM protocols and ports

Nokia recommends using a strict CPM management access filter policy allowing traffic from trusted IP subnets for protocols and ports actively used in the router and to explicitly drop other traffic.

The following table identifies the protocols and TCP/UDP ports used per application on 7210 SAS platforms. The source port and destination port reflect the CPM management access filter entry configuration for traffic ingressing the router and sent to the CPM.

Table 7: Protocols and TCP/UDP ports used by applications on 7210 SAS platforms

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
BFD application															
	3784	UDP	BFD control 1 hop BFD	✓				✓		✓		✓		✓	
	3785	UDP	BFD echo	✓				✓		✓		✓		✓	
	4784	UDP	BFD control multi-hop	✓				✓		✓		✓		✓	
	6784	UDP	Micro-BFD	✓				✓		✓		✓		✓	
BGP application															
	179	TCP	BGP: server terminated	✓				✓		✓		✓		✓	

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
			TCP sessions												
179		TCP	BGP: client responses for initiated TCP session	✓				✓		✓		✓		✓	
Cflowd application															
	1025 to 65535	UDP						✓	✓	✓[10]	✓[10]	✓	✓		
DHCPv4 application															
67	67	UDP	DHCPv4: relay agent to server; server to relay agent; relay agent to relay agent	✓		✓		✓		✓		✓		✓	
68	67	UDP	DHCPv4: client to relay agent; client to server	✓		✓		✓		✓		✓		✓	
67	68	UDP	DHCPv4: relay agent to server; relay agent to client	✓		✓		✓		✓		✓		✓	

[10] On the 7210 SAS-R, the cflowd application is only supported on the 7210 SAS-R6.

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/S 1/10GE		SAS-Sx 10/100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
DHCPv6 application															
546	547	UDP	DHCPv6: client to server; client to relay agent					✓							
547	546	UDP	DHCPv6: server to relay agent; relay agent to server; relay agent to relay agent					✓							
DNS application															
53		UDP	DNS Client	✓		✓		✓		✓		✓		✓	
FTP application															
	20	TCP	FTP server data and active FTP client	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	21	TCP	FTP server control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
20		TCP	FTP client data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
21		TCP	FTP client control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
GRE application															

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
N/A	N/A	GRE	GRE	✓				✓		✓		✓		✓	
ICMP application															
N/A	N/A	ICMP	ICMP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP application															
N/A	N/A	IGMP	IGMP	✓		✓		✓		✓		✓		✓	
LDP application															
	646	UDP	LDP hello adjacency	✓				✓		✓		✓		✓	
	646	TCP	LDP/T-LDP: terminated TCP sessions	✓				✓		✓		✓		✓	
646		TCP	LDP/T-LDP: responses for initiated TCP sessions	✓				✓		✓		✓		✓	
MC-APS application															
	1025	UDP	Multi-chassis LAG	✓		✓		✓		✓		✓		✓	
MCS application															
	45067	TCP	Multi-chassis synchronization: terminated TCP session	✓		✓		✓		✓		✓		✓	
45067		TCP	Multi-chassis	✓		✓		✓		✓		✓		✓	

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
			synchronization: responses for initiated TCP session												
NETCONF application															
	830	TCP	NETCONF							✓					
NTP application															
	123	UDP	NTP server	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
123		UDP	NTP client	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OAM application															
	3503	UDP	LSP ping	✓				✓		✓		✓		✓	
	33408 to 33535	UDP	OAM traceroute	✓				✓		✓		✓		✓	
OSPF application															
N/A	N/A	OSPF	OSPF	✓				✓		✓		✓		✓	
PCEP application															
	4189	TCP	Path Computation Element Protocol (PCEP)					✓	✓	✓	✓				
PIM application															
	3232	UDP	PIM MDT	✓				✓		✓		✓		✓	
N/A	N/A	PIM	PIM	✓				✓		✓		✓		✓	

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
PTP application															
	319	UDP	1588 PTP event	✓		✓		✓		✓		✓		✓	
	320	UDP	1588 PTP general	✓		✓		✓		✓		✓		✓	
RADIUS application															
1812		UDP	Radius authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1813		UDP	Radius accounting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RIP application															
	520	UDP	RIP (only on SAS-Mxp)					✓							
RSVP application															
N/A	N/A	RSVP	RSVP	✓				✓		✓		✓		✓	
SSH application															
	22	TCP	SSH server and terminated TCP session	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
22		TCP	SSH client and responses for initiated TCP sessions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SNMP application															

TCP/UDP port number		IP protocol	Application description	Protocols and ports available for in-band and out-of-band management on 7210 SAS platforms											
				SAS-T (network mode)		SAS-T (access-uplink mode)		SAS-MXP		SAS-R6 and SAS-R12		SAS-Sx/ S 1/10GE		SAS-Sx 10/ 100GE	
Source	Destination			In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band	In-band	Out-of-band
	161	UDP	SNMP server; SET and GET commands	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TACACS application															
49		TCP	TACACS client and responses for initiated TCP sessions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TELNET application															
	23	TCP	TELNET server	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TWAMP application															
	862	TCP	TWAMP control: terminated TCP session	✓		✓		✓		✓		✓		✓	
	Any	UDP	TWAMP test	✓		✓		✓		✓		✓		✓	
	1 to 65535	UDP	TWAMP light (per router instance)	✓		✓		✓		✓		✓		✓	
VRRP application															
N/A	N/A	VRRP	VRRP	✓				✓		✓		✓		✓	

2.3.2 Management Access Filter

Management Access Filters (MAF) are software-based filters used to restrict traffic extracted from the data plane and restrict traffic from the management port to the CPU.

2.3.2.1 MAF packet match

Two different **management-access-filter** policies can be configured: **ip-filter** and **ipv6-filter**.

The following are the MAF packet match rules:

- Each MAF policy is an ordered list of entries; therefore, entries must be sequenced correctly from the most to the least explicit.
- If multiple match criteria are specified in a single MAF policy entry, all criteria must be met for the packet to be considered a match against that policy entry (logical AND).
- Any match criteria not explicitly defined is ignored during a match.
- A MAF filter policy entry defined without a match criteria is inactive.
- A MAF filter policy entry with match criteria defined but no action configured inherits the default action defined at the **management-access-filter** level.
- The **management-access-filter default-action** applies individually per IPv4 or IPv6 filter policies that are in a **no shutdown** state.

2.3.2.2 MAF IPv4/IPv6 filter entry match criteria

The following table lists the supported IPv4 and IPv6 match criteria.

Table 8: IPv4 and IPv6 match criteria

Criteria	Description
dst-port	Matches the specified port value against the destination port number of the UDP or TCP packet header.
flow-label	Matches the IPv6 flow label.
fragment	Matches fragmented or non-fragmented IP packet.
next-header	Matches the specified upper-layer protocol (such as TCP, UDP, or IGMPv6) against the next-header field of the IPv6 packet header. "*" can be used to specify a TCP or UDP upper-layer protocol match (logical OR). Next-header matching also allows matching on presence of a subset of IPv6 extension headers. See Management Access Filter commands for details about which extension header match is supported.
l4-source-port	Matches the specified port value against the L4 source port number of the UDP or TCP packet header.
protocol	Matches the specified protocol against the Protocol field in the IPv4 packet header (for example, TCP, UDP, or IGMP) of the outer IPv4.

Criteria	Description
	"*" can be used to specify TCP or UDP upper-layer protocol match (logical OR).
router	Matches the router instance that packets are ingressing from for this filter entry.
src-ip	Matches the specified source IPv4 or IPv6 address prefix and mask against the source IPv4 or IPv6 address field in the IP packet header.
src-port	Matches packets that are ingressing from this port.

2.3.2.3 MAF policy action

MAFs allow actions to **permit** or **deny** (or use the **deny-host-unreachable** response for IP filters) traffic.

2.3.2.4 MAF policy statistics and logging

The management access filter match count can be displayed using **show** commands. Logging is recorded in the system security logs.

2.4 CPU protection modes

The 7210 SAS provides several rate limiting mechanisms to protect the CPM/CFM processing resources of the router:

- Centralized CPU Protection: a centralized rate-limiting function that operates on the CPM to limit traffic destined to the CPUs. The CPU protection mechanism is not user-configurable. It is supported on all 7210 SAS platforms.

  For historical reasons, the term "centralized CPU protection" is called "CPU protection" in this user guide.

- Distributed CPU Protection (DCP): a control traffic rate-limiting protection mechanism for the CPM and CFM that operates on line cards. See DCP for more information about the DCP mechanism.

2.4.1 Centralized CPU protection

The CPU protection mechanism protects the CPU from a DoS attack by limiting the amount of ingress port traffic destined for the CPM to be processed by its CPU. On the 7210 SAS, a set of dedicated policers are used to limit the amount of traffic to the software-defined rate (the rate is not user-configurable) before the packets are queued to the CPU queues. A strict policy scheduler schedules packets from the CPU queues. A CPU queue traffic shaper, configured to a predefined rate by software, is used to limit the amount of traffic for a protocol or group of protocols using the CPU queue.

In most cases, access interfaces and network uplinks do not share the policers and CPU queues used to manage the amount of traffic sent to the CPM. Access interfaces (typically used to deliver customer

services) use a dedicated set of policers and CPU queues; a separate set is used for network facing ports (that is, network ports, hybrid ports, and access-uplink ports). The policer rate and CPU queue rates used for CPU protection are not user-configurable.

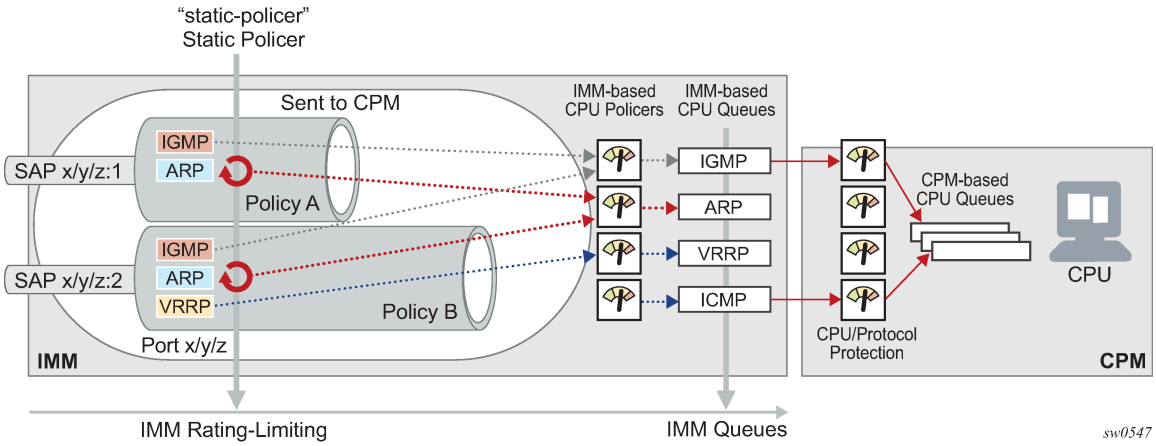
2.4.2 DCP

DCP provides a powerful per-protocol-per-object rate-limiting function for control protocol traffic that is extracted from the datapath and sent to the CPM. See DCP applicability for a list of applicable objects. The DCP function is implemented on the router for granular control.

DCP provides the enforcement policers to configure policies that are applied to objects (for example, SAPs). An enforcement policer is an instance of a policer that is policing a flow of packets composed of a single protocol arriving on a single object (for example, SAP). Enforcement policers perform a configurable action, such as a discard, on packets that exceed the configured rate parameters. Static policers are the one type of enforcement policer supported on the 7210 SAS-R6 and 7210 SAS-R12, which are always instantiated if configured.

The following figure shows per-SAP per-protocol static rate limiting with DCP.

Figure 3: Per-SAP per-protocol static rate limiting with DCP



Note:
CPU policers and CPU queues on CPM and IMM are shown only for some protocols. on the 7210 SAS, all control traffic to the CPU is rate-limited using a policer per protocol or group of protocols. The CPU queues are further shaped to the system-defined rate. There are different policers and queues used for access ports and network ports to ensure that customer traffic does not affect critical network traffic. The rates for these CPU policers and queues are not configurable by the user.

2.4.2.1 DCP applicability

By default, the system does not associate a DCP policy with a SAP. The user must configure an explicit policy to enable DCP for a SAP for a supported protocol. Allocate resources for the DCP policy from the ingress internal TCAM resource pool by using the **configure>system>resource-profile>ingress-internal-tcam>cpu-protection** command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information about this command.

The DCP functionality is not enabled on the service objects by default. Use the **dist-cpu-protection** command in the **config**>**service** context to enable the DCP functionality on service objects. The **no** form of the command disables the DCP functionality on service objects.

DCP policies can be applied to the following types of objects:

- IES SAP
- VPRN SAP
- RVPLS SAP

For RVPLS, DCP rate-limits the packets arriving at the CPU, but for flooded traffic, ingress QoS or ACLs must be used.

Control packets that are extracted in an IES or a VPRN service, where the packets arrived into the node over a VPLS SAP (that is, R-VPLS scenario), will use the DCP policy and policer instances associated with the VPLS SAP. In this case, a DCP policy created for VPLS SAPs, for VPLSs that have a Layer 3 interface bound to them (R-VPLS), may have protocols such as ARP configured in the policy.

2.4.2.2 Log events, statistics, status and SNMP support

Log events are supported for DCP to warn against potential attacks or misconfigurations, and to tune DCP settings. DCP throttles the rate of DCP events to avoid event floods when multiple parallel attacks or problems occur in the system.

Most DCP log events can be enabled or disabled both individually at the DCP policy level (in the DCP policy configuration), and globally in the system (in log event control).

In the case where the DCP log event indicates a SAP that is an MSAP, the operator can identify the subscribers on a specific MSAP by using the **show service active-subscriber** command and filtering ("| match") on the MSAP string.

The DCP statistics and status is available via the following:

- **SNMP**

  For detailed information, see the tables and NOTIFICATION-TYPE objects in the following MIBs where "Dcp" or "DCpuProt" occurs in the applicable object name:

  – TIMETRA-CHASSIS-MIB
  – TIMETRA-SAP-MIB
  – TIMETRA-VRTR-MIB
  – TIMETRA-SECURITY-MIB

- **CLI**

  Use the **show log event-control** | **match Dcp** command to display the log events in the CLI.

  In the case where the DCP log event indicates a SAP that is an MSAP, the operator can identify the subscribers on a specific MSAP by using the **show service active-subscriber** command and filtering ("| match") on the MSAP string.

2.4.2.3 DCP policer resource management

CAM and meter resources from the CPU protection pool are allocated for the DCP policer by using the **configure**>**system**>**resource-profile**>**ingress-internal-tcam**>**cpu-protection** command. Resources

from this pool (also called a slice) are also used to identify protocol packets that need to be rate-limited and have used a policer or meter to the configured rate before being queued to the CPU queues. Two CAM entries with a single policer is used for every protocol configured in the DCP policy. The 7210 SAS does not support sharing of a policer among protocols. All protocols configured to use a policer are allocated an independent instance of the policer and are policed to the configured rate. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for information about resource allocation using the **cpu-protection** CLI command.

2.4.2.4 Operational guidelines

This section describes the operational guidelines to leverage distributed CPU protection:

- To completely block a set of specific protocols on a specific SAP, create a single static policer with a rate of 0 and map the protocols to that policer.
- During normal operation, Nokia recommends that log events for state policers should be configured using the **log-events** command without the optional **verbose** keyword. Use the **verbose** keyword selectively during debugging, testing, tuning, and investigation.
- Every protocol configured to use a policer is allocated an independent policer instance to rate-limit that protocol. A single policer cannot be shared across multiple protocols. For example, if a single policer is configured in the service and there are four protocols configured to use it, four policer instances are allocated (that is, eight CAM entries are used for identifying the protocol and four meters are allocated).
- The rates enforced by centralized CPU protection are also enforced for protocols configured for DCP. That is, DCP allows users to enforce rates per service object to be below the system-defined rate of the centralized CPU protection. Therefore, it prevents customer traffic from affecting other customer traffic.

2.5 Vendor-specific attributes (VSAs)

The 7210 SAS supports the configuration of Nokia-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are described 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.

The PE-record entry is required to support the RADIUS Discovery for Layer 2 VPN feature. 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:

The **authentication-order** parameters configured on the router must include the **local** keyword.

The username may or may not be configured on the router.

The user must be authenticated by the RADIUS server

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 preceding 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 system exits on the first match; subordinate levels cannot be modified with subsequent action commands. Subordinate level VSAs must be entered before 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:

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

If all of the preceding conditions 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.

2.5.1 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. The "ruser1" 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.

Example

```
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,
```

2.6 Other security features

This sections describes security features supported on the 7210 SAS.

2.6.1 Security algorithms

The following table lists the security algorithms supported per protocol.

Table 9: Security algorithm support per platform

Protocol	Clear text	MD5	HMAC-MD5	HMAC-SHA1-96	HMAC-SHA1	HMAC-SHA256	AES-128-CMAC-96
OSPF	✓	✓		✓	✓	✓	
IS-IS	✓		✓		✓	✓	
RSVP	✓		✓		✓		
BGP				✓			✓
LDP		✓		✓			✓

2.6.2 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.

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

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

The 7210 SAS 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 the SSH server is enabled, an SSH security key is generated. Unless the **perserve-key** command option is configured for SSH, the security key is only valid until the node is restarted or the SSH server is stopped and restarted. The key size is non-configurable and set to 2048 for SSHv2 RSA, and to 1024 for SSHv2 DSA and SSHv1 RSA. When the server is enabled, both inbound SSH and SCP sessions are accepted, as long as the session is properly authenticated.

When the global SSH server process is disabled, no inbound SSH or SCP sessions are 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 interpret the backslash character as an "escape" character, which is not 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 be used to properly delimit directories and the filename.

2.6.3 SSH PKI authentication

The SSH server supports a public key authentication provided that the server has been previously configured to know the client's public key.

Using public key authentication, also known as Public Key Infrastructure (PKI), can be more secure than the existing username and password method because of the following:

- A user typically reuses the same password with multiple servers. If the password is compromised, the user must reconfigure the password on all affected servers.
- A password is not transmitted between the client and server using PKI. Instead the sensitive information (the private key) is kept on the client. Consequently, the password is less likely to be compromised.

The 7210 SAS supports server-side SSHv2 public key authentication, but does not include a key-generation utility.

PKI should be configured in the system-level configuration where one or more public keys may be bound to a username. This configuration does not affect any other system security or login functions.

PKI has preference over password or keyboard authentication. PKI is supported using only local authentication. PKI authentication is not supported on TACACS+ or RADIUS.

2.6.3.1 User public key generation

Before SSH can be used with PKI, the client must generate a public/private key pair. This is typically supported by the SSH client software. For example, PuTTY supports a utility called PuTTYGen that generates key pairs.

The 7210 SAS currently supports only Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys.

If the SSH client software uses PuTTY, it must first generate a key pair using PuTTYGen. The client sets the key type to SSH-2 RSA and configures the number of bits to be used for the key. The client can also configure a passphrase to store the key locally in encrypted form. If the passphrase is configured, it acts as a password that the client must enter to use the private key. If a passphrase is not configured, the private key is stored in plain text locally.

Next, use the **config**>**system**>**security**>**user**>**public-keys** command to configure the public key for the client (the public key is obtained as part of the key pair). On the 7210 SAS, the user can program the public key using CLI commands (accessed through Telnet/SSH) or SNMP.

Note:
The preceding process to generate a key pair is an example only. This process is not executed on a 7210 SAS node, but on a third-party node acting as the SSH client or any other node.

2.6.4 MAC client and server list

The 7210 SAS supports a configurable client and server MAC list for SSHv2, which allows the user to add or remove Message Authentication Code (MAC) algorithms from the list. The user can program the strong Hashed Message Authentication Code (HMAC) algorithms on top of the configurable MAC list (for example, lowest index in the list) to be negotiated first between the client and server. The first algorithm in the list that is supported by both the client and the server is the one that is agreed upon.

There are two configurable MAC lists:

- client list
- server list

The default client and server MAC list includes all supported algorithms in the following preference order:

1. mac 200 name hmac-sha2-512
2. mac 210 name hmac-sha2-256
3. mac 215 name hmac-sha1
4. mac 220 name hmac-sha1-96
5. mac 225 name hmac-md5
6. mac 230 name hmac-ripemd160
7. mac 235 name hmac-ripemd160-openssh-com
8. mac 240 name hmac-md5-96

Note:
The configurable MAC list is only supported for SSHv2 and not for SSHv1. SSHv1 only supports 32-bit CRC.

2.6.5 Cipher client and server list

The 7210 SAS supports cipher client and server lists. The user can add or remove the desired SSH cipher client and server algorithms to be negotiated. The list is an index list with the lower index having higher preference in the SSH negotiation. The lowest index algorithm in the list is negotiated first in SSH connections and is on top of the negotiation list to the peer.

There is a separate cipher list for SSHv1 and SSHv2 for both client and server.

The default client cipher list for SSHv1 includes all supported algorithms in the following preference order:

1. cipher 200 name 3des
2. cipher 205 name blowfish
3. cipher 210 name des

The default server cipher list for SSHv1 includes algorithms in the following preference order:

1. cipher 200 name 3des
2. cipher 205 name blowfish

The default server and client lists for SSHv2 include all supported algorithms in the following preference order:

1. cipher 190 name aes256-ctr

2. cipher 192 name aes192-ctr
3. cipher 194 name aes128-ctr
4. cipher 200 name aes128-cbc
5. cipher 205 name 3des-cbc
6. cipher 210 name blowfish-cbc
7. cipher 215 name cast128-cbc
8. cipher 220 name arcfour
9. cipher 225 name aes192-cbc
10. cipher 230 name aes256-cbc
11. cipher 235 name rijndael-cbc

Use the following CLI syntax to configure the client and server cipher list.

```
configure system security ssh client-cipher-list
  client-cipher-list protocol-version <version>
 <version>            : [1..2]
configure system security ssh client-cipher-list cipher
  cipher <index> name <cipher-name>
  no cipher <index>
 <index>              : [1..255]
 <cipher-name>        : aes128-ctr|aes192-ctr|aes256-ctr|des|3des|blowfish|
                        3des-cbc|blowfish-cbc|cast128-cbc|arcfour|aes128-cbc|
                        aes192-cbc|aes256-cbc|rijndael-cbc
configure system security ssh server-cipher-list
  server-cipher-list protocol-version <version>
 <version>            : [1..2]
configure system security ssh server-cipher-list cipher
  no cipher <index>
  cipher <index> name <cipher-name>
 <index>              : [1..255]
 <cipher-name>        : aes128-ctr|aes192-ctr|aes256-ctr|des|3des|blowfish|
                        3des-cbc|blowfish-cbc|cast128-cbc|arcfour|aes128-cbc|
                        aes192-cbc|aes256-cbc|rijndael-cbc
```

2.6.6 KEX client and server list

The 7210 SAS supports key exchange (KEX) client and server lists. The user can add or remove the KEX client or server algorithms that the SSH application negotiates using an SSHv2 phase one handshake. The KEX list is an index list with the lower index having higher preference in the SSH negotiation. The lowest indexed algorithm in the list is negotiated first in SSH and is at the top of the negotiation list to the peer.

By default, the KEX list is empty and a hard-coded list that includes all supported algorithms in the following preference order is used:

1. kex 200 name diffie-hellman-group16-sha512
2. kex 210 name diffie-hellman-group14-sha256
3. kex 215 name diffie-hellman-group14-sha1
4. kex 220 name diffie-hellman-group-exchange-sha1
5. kex 225 name diffie-hellman-group1-sha1

As soon as the user configures the KEX list, the 7210 SAS starts using the algorithms from the user-defined KEX list instead of the hard-coded list. To revert to the hard-coded list, the user must remove all configured KEX indexes until the list is empty.

Use the following CLI to configure the cipher or MAC server and client lists.

```
configure system security ssh server-kex-list kex
   kex <index> name <kex-name>
   no kex <index>

configure system security ssh client-kex-list kex
   kex <index> name <kex-name>
   no kex <index>

<index>              : [1..255]
<kex-name>           : diffie-hellman-group14-sha1| diffie-hellman-group14-sha256|
                       diffie-hellman-group16-sha512|diffie-hellman-group-exchange-
                       sha1| diffie-hellman-group1-sha1
```

2.6.7 Exponential login backoff

A malicious user may attempt to gain CLI access by means of a dictionary attack, in which a script is used to attempt automatic logins as an "admin" user and a dictionary list is used to test all possible passwords. By 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 attempts to log into a router using a Telnet or an SSH session, the system allows a limited number of attempts to enter the correct password. The interval between the unsuccessful attempts change after each try (1, 2, and 4 seconds). If user lockout is configured on the system, the user will be locked out when the number of unsuccessful attempts is exceeded.

However, if lockout is not configured, three password entry attempts are allowed in the first session after the first failure, at fixed 1, 2 and 4 second intervals, 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 terminates after four unsuccessful attempts. A wait period is never longer than 4 seconds. The periods are fixed and restart in subsequent sessions.

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.

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.

See Configuring login controls. The commands are described in Login, Telnet, SSH and FTP commands.

2.6.8 User lockout

When a user exceeds the maximum number of attempts allowed (the default is 3 attempts) during a specific period of time (the default is 5 minutes) the account used during those attempts will be locked out for a preconfigured 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.

2.6.9 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.

2.6.10 802.1x network access control

The 7210 SAS supports network access control of client devices (PCs, STBs, and so on) 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.

2.6.11 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.

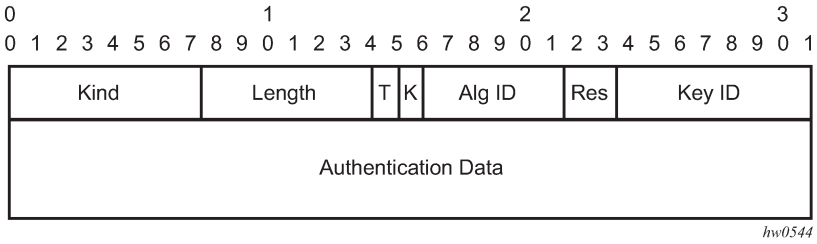
The TCP Enhanced Authentication Option is a TCP extension that enhances security for BGP, LDP and other TCP-based protocols. This includes the ability to change keys in a BGP or LDP session seamlessly without tearing down the session. It is intended for applications where secure administrative access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

2.6.11.1 Packet formats

The following figure shows the packet format for the Enhanced Authentication Option.

Figure 4: Packet formats



Option Syntax:

- **Kind: 8 bits**

  The Kind field identifies the TCP Enhanced Authentication Option. This value will be assigned by IANA.

- **Length: 8 bits**

  The Length field specifies the length of the TCP Enhanced Authentication Option, in octets. This count includes two octets representing the Kind and Length fields.

  The valid range for this field is from 4 to 40 octets, inclusive.

  For all algorithms specified in this memo the value will be 16 octets.

- **T-Bit: 1 bit**

  The T-bit specifies whether TCP Options were omitted from the TCP header for the purpose of MAC calculation. A value of 1 indicates that all TCP options other than the Extended Authentication Option were omitted. A value of 0 indicates that TCP options were included.

  The default value is 0.

- **K-Bit: 1 bit**

  This bit is reserved for future enhancement. Its value MUST be equal to zero.

- **Alg ID: 6 bits**

  The Alg ID field identifies the MAC algorithm.

- **Res: 2 bits**

  These bits are reserved. They MUST be set to zero.

- **Key ID: 6 bits**

  The Key ID field identifies the key that was used to generate the message digest.

- **Authentication Data: Variable length**

  The Authentication Data field contains data that is used to authenticate the TCP segment. This data includes, but need not be restricted to, a MAC. The length and format of the Authentication Data Field can be derived from the Alg ID.

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

2.6.11.2 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 described in the following table.

Table 10: 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).
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**

Field	Definition	CLI
		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**

2.7 Configuration notes

This section describes security configuration guidelines and caveats.

2.7.1 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.

2.8 Configuring security with CLI

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

2.8.1 Setting up security attributes

This section provides a brief overview of the tasks that must be performed to configure security and provides the CLI commands. The following table describes 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 11: Security configuration requirements

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

2.8.1.1 Configuring authentication

See the following sections to configure authentication:

- Local authentication
  - Configuring password management parameters
  - Configuring profiles
  - Configuring users
- RADIUS authentication (only)

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

  To implement only RADIUS authentication, with authorization, perform the following tasks on each participating router:
  - Configuring RADIUS authentication
  - Configuring RADIUS authorization
- TACACS+ authentication

  To implement only TACACS+ authentication, perform the following tasks on each participating router:
  - Configuring profiles
  - Configuring users
  - Enabling TACACS+ authentication

2.8.1.2 Configuring authorization

See the following sections to configure authorization:

- Local authorization

  For local authorization, configure these tasks on each participating router:
  - Configuring profiles
  - Configuring users
- RADIUS authorization (only)

  For RADIUS authorization (without authentication), configure these tasks on each participating router:
  - Configuring RADIUS authorization
  - Configuring profiles

  For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-specific attributes (VSAs).
- RADIUS authorization

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

  - Configuring RADIUS authorization For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-specific attributes (VSAs).
  - Configuring RADIUS authentication
  - Configuring profiles
- TACACS+ authorization (only)

  For TACACS+ authorization (without authentication), configure these tasks on each participating router:
  - Configuring TACACS+ authorization
- TACACS+ authorization

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

2.8.1.3 Configuring accounting

The following sections provide information about configuring accounting.

2.8.2 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

Example

The following are sample 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
```

2.8.3 Security configuration procedures

The following sections provide information about configuring security components.

2.8.3.1 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 keyword CPM to be considered complete. Entries without the action keyword are considered incomplete and will be rendered inactive.

Use the following syntax 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.

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

2.8.3.2 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 syntax to configure password support.

```
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-rules
                allow-user-name
                credits [lowercase credits] [uppercase credits] [numeric credits] [special-
character credits]
                minimum-classes minimum
                minimum-length length
                repeated-characters count
                required [lowercase count] [uppercase count] [numeric count] [special-
character count]
            hashing {bcrypt|sha2-pbkdf2}
            health-check [interval interval]
            history-size size
            minimum-age [days days] [hrs hours] [min minutes] [sec seconds]
```

```
            minimum-change distance
```

Example: Password configuration output

```
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#
```

2.8.3.3 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 syntax to configure user profiles.

```
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}
```

Example: User profile configuration 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#
```

2.8.3.4 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 syntax to configure RADIUS support.

```
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} privacy {none|des-key key-2}]}
        group group-name
```

Example: User configuration output

```
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#
```

2.8.3.5 Configuring keychains

Example: Keychain configuration output

```
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#
```

2.8.3.6 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.

2.8.3.6.1 User

Use the following CLI syntax to copy a user.

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

Example: Command usage

```
  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#
```

Example: Copied user configuration output

```
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
```

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

Example

```
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#
```

2.8.3.6.2 Profile

Use the following CLI syntax to copy a profile.

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

Example: Command usage

```
config>system>security# copy profile default to testuser
```

Example: Copied profiles configuration output

```
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#
```

2.8.3.7 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.

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

Example

The following is a sample SSH server configuration output 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#
```

2.8.4 RADIUS configurations

The following sections provide information about configuring RADIUS functionality.

2.8.4.1 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*.

The system IP address must be configured in order for the RADIUS client to work.

The other commands are optional. The server command adds a RADIUS server and configures the RADIUS server 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 syntax to configure RADIUS authentication.

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

Example: RADIUS authentication configuration output

```
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#
```

2.8.4.2 Configuring RADIUS authorization

In order for RADIUS authorization to function, RADIUS authentication must be enabled first. See Configuring RADIUS authentication.

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See Vendor-specific attributes (VSAs).

On the local router, use the following syntax to configure RADIUS authorization.

```
config>system>security
    radius
    authorization
```

Example: RADIUS authorization configuration output

```
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#
```

2.8.4.3 Configuring RADIUS accounting

Use the following syntax to configure RADIUS accounting on a local router.

```
config>system>security
        radius
            accounting
```

Example: RADIUS accounting configuration output

```
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#
```

2.8.4.4 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. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide*.

To configure generic parameters for 802.1x authentication, enter the following 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
```

Example: 802.1x configuration output

```
A:ALA-1>config>system>security# info
----------------------------------------------
            dot1x
                radius-plcy "dot1x_plcy" create
                   server 1 address 10.1.1.1 port 65535 secret "a"
                   server 2 address 10.1.1.2 port 6555 secret "a"
                   source-address 10.1.1.255
                no shutdown
...
----------------------------------------------
A:ALA-1>config>system#
```

2.8.5 TACACS+ configurations

2.8.5.1 Enabling TACACS+ authentication

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

Use the following syntax to configure profiles.

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

Example: TACACS+ authentication configuration output

```
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#
```

2.8.5.2 Configuring TACACS+ authorization

In order for TACACS+ authorization to function, TACACS+ authentication must be enabled first. See Enabling TACACS+ authentication.

Use the following syntax to configure RADIUS authorization on the local router.

```
config>system>security
        tacplus
            authorization
            no shutdown
```

Example: TACACS+ authorization configuration output

```
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#
```

2.8.5.3 Configuring TACACS+ accounting

Use the following syntax to configure TACACS+ accounting on a local router.

```
config>system>security
        tacplus
            accounting
```

Example: TACACS+ accounting configuration output

```
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#
```

2.8.6 Configuring login controls

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

Use the following syntax to configure login controls.

```
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}
```

Example: Login control configuration output

```
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 prohibited."
           motd text "Notice to all users: Software upgrade scheduled 3/2 1:00 AM"
       exit
 no exponential-backoff
...
-----------------------------------------------
A:ALA-1>config>system#
```

2.9 Security command reference

2.9.1 Command hierarchies

- Configuration commands
  - Security commands
  - Management Access Filter commands
  - Distributed CPU protection commands
  - Security password commands
  - Profile commands
  - RADIUS commands
  - SSH commands
  - TACPLUS commands
  - User commands
  - User template commands
  - Dot1x commands
  - Keychain commands
  - Login control commands
  - IPsec commands
- Show commands
- Clear commands
- Debug commands

2.9.1.1 Configuration commands

2.9.1.1.1 Security commands

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

2.9.1.1.2 Management Access Filter commands

```
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
```

2.9.1.1.3 Distributed CPU protection commands

```
config
    - system
        - security
            - dist-cpu-protection
                - policy policy-name [create]
                - no policy policy-name
                    - description description-string
                    - no description
                    - protocol name [create]
                    - no protocol name
                        - enforcement {static policer-name}
                    - static-policer policer-name [create]
                    - no static-policer policer-name
                        - description description-string
                        - no description
                        - exceed-action {discard | none}
                        - log-events [verbose]
                        - no log-events
                        - rate {kbps {kilobits-per-second | max} {[mbs size] [bytes |
 kilobytes]}
                        - no rate
```

2.9.1.1.4 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
                - hashing  {bcrypt | sha2-pbkdf2}
                - [no] health-check [interval interval]
                - history  size
                - no history
                - minimum-age [days days] [hrs hours] [min minutes] [sec seconds]
                - no minimum-age
                - minimum-change distance
                - no minimum-change
```

2.9.1.1.5 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
```

2.9.1.1.6 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
```

2.9.1.1.7 SSH commands

```
config
    - system
        - security
            - ssh
                - client-cipher-list protocol-version version
                    - cipher index name cipher-name
                    - no cipher index
                - client-mac-list
                    - mac index name mac-name
                    - no mac index
                - client-kex-list
                    - kex  index name kex-name
                    - no kex  index
                - [no] preserve-key
                - server-cipher-list protocol-version version
                    - cipher index name cipher-name
                    - no cipher index
                - server-mac-list
                    - mac index name mac-name
                    - no mac index
                - server-kex-list
                    - kex  index name kex-name
                    - no kex  index
                - [no] server-shutdown
                - [no] version ssh-version
```

2.9.1.1.8 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
```

2.9.1.1.9 User commands

```
config
    - system
        - security
```

```
            - [no] user user-name
                - [no] access [ftp] [snmp] [console]
                - console
                    - [no] cannot-change-password
                    - login-exec url-prefix:source-url
                    - no login-exec
                    - [no] member user-profile-name [user-profile-name…(up to 8 max)]
                    - [no] new-password-at-login
                - home-directory url-prefix [directory] [directory/directory…]
                - no home-directory
                - password [password] [hash | hash2]
                - public-keys
                    - ecdsa
                        - ecdsa-key ecdsa-public-key-id [create]
                        - no ecdsa-key ecdsa-public-key-id
                            - description description-string
                            - no description
                            - key-value ecdsa-public-key-value
                            - no key-value
                    - rsa
                        - rsa-key rsa-public-key-id [create]
                        - no rsa-key rsa-public-key-id
                            - description description-string
                            - no description
                            - key-value rsa-public-key-value
                            - no key-value
                - [no] restricted-to-home
                - snmp
                    - authentication none
                    - authentication authentication authentication-protocol key-1 [privacy
none] [hash | hash2]
                    - authentication authentication authentication-protocol key-1
privacy privacy-protocol key-2 [hash | hash2]
                    - no authentication
                    - group group-name
                    - no group
```

2.9.1.1.10 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
                - profile user-profile-name
                - no profile
                - [no] restricted-to-home
```

2.9.1.1.11 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
```

2.9.1.1.12 Keychain commands

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

2.9.1.1.13 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
```

2.9.1.1.14 IPsec commands

```
config
    - ipsec
        - static-sa sa-name
        - no static-sa
            - authentication auth-algorithm ascii-key ascii-string
            - authentication auth-algorithm hex-key hex-string [hash | hash2]
            - no authentication
            - description description-string
            - no description
            - direction ipsec-direction
            - no direction
            - protocol ipsec-protocol
            - no protocol
            - spi spi
            - no spi
```

2.9.1.2 Show commands

2.9.1.2.1 Security

```
show
    - system
        - security
            - access-group [group-name]
            - authentication [statistics]
            - dist-cpu-protection
```

```
                - policy [name] [association | detail]
            - 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-name] [detail]
            - view [view-name] [detail]
```

2.9.1.2.2 Login control

```
show
    - users
```

2.9.1.3 Clear commands

```
admin
    - user user-name
        - lockout
```

2.9.1.4 Debug commands

```
debug
    - router
        - radius
        - no radius
            - detail-level {low | medium | high}
            - no detail-level
            - packet-type [authentication] [accounting] [coa]
            - no packet-type
            - radius-attr type attribute-type [transaction]
            - radius-attr type attribute-type [transaction] {address | hex | integer | string}
 value attribute-value
            - radius-attr vendor vendor-id type attribute-type [transaction]
 [encoding encoding-type]
            - radius-attr vendor vendor-id type attribute-type [transaction]
 [encoding encoding-type] {address | hex | integer | string} value attribute-value
            - no radius-attr type attribute-type
            - no radius-attr type attribute-type {address | hex | integer | string}
 value attribute-value
            - no radius-attr vendor vendor-id type attribute-type
            - no radius-attr vendor vendor-id type attribute-type {address | hex | integer |
 string} value attribute-value
            - server-address ip-address
            - no server-address ip-address
```

2.9.2 Command descriptions

- Configuration commands
- Show commands
- Debug commands

2.9.2.1 Configuration commands

- General security commands
- Login, Telnet, SSH and FTP commands
- Management Access Filter commands
- Password commands
- Profile management commands
- User management commands
- RADIUS client commands
- TACACS+ client commands
- Generic 802.1x commands
- TCP Enhanced Authentication commands

2.9.2.1.1 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

config>system>security>user>public-keys>ecdsa>ecdsa-key

config>system>security>user>public-keys>rsa>rsa-key

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 this command removes the string.

Parameters

string

The description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This 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 this command puts an entity into the administratively enabled state.

Default

no shutdown

security

Syntax

security

Context

config>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command disables FTP servers running on the system.

Default

no ftp-server

hash-control

Syntax

hash-control [**read-version** {**1** | **2** | **all**}] [**write-version** {**1** | **2**}]

no hash-control

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables the system to encrypt all passwords, MD5 keys, and so on using specific algorithms.

Whenever the user executes a **save** or **info** command, the system will encrypt all passwords, MD5 keys, and so on 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 needs 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

Parameters

read-version {1 | 2 | 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context specify 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 the source IP address. That is, 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the application to use the source IPv4 address specified by the **source-address** command.

Parameters

app

Specifies the application name.

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

Note:
PTP is supported on all 7210 SAS platforms as described in this document, except the 7210 SAS-S 1/10GE. Only applications supported on a 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 and IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

application6

Syntax

application6 *app* [*ipv6-address*]

no application6 *app*

Context

config>system>security>source-address

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the application to use the source IPv6 address specified by the source address.

Parameters

app

Specifies the application name.

Values dns | ftp | ping | radius | snmptrap | syslog | tacplus | telnet | traceroute

ipv6-address

Specifies the name of the IPv6 address.

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

telnet-server

Syntax

[**no**] **telnet-server**

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 client to three login attempts. The Telnet server disconnects the Telnet client session after the third attempt.

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

2.9.2.1.2 Login, Telnet, SSH and FTP commands

exponential-backoff

Syntax

[**no**] **exponential-backoff**

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command disables exponential backoff.

Default

no exponential-backoff

ftp

Syntax

ftp

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure FTP login control parameters.

idle-timeout

Syntax

idle-timeout {*minutes* | **disable**}

no idle-timeout

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

idle-timeout 30

Parameters

minutes

Specifies the idle timeout in minutes. Allowed values are 1 to 1440. A value of 0 implies that the sessions never timeout.

Values 1 to 1440

disable

Keyword to specify that 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

3

Parameters

value

Specifies the maximum number of concurrent FTP sessions on the node.

Values 0 to 5

inbound-max-sessions

Syntax

inbound-max-sessions *value*

no inbound-max-sessions

Context

config>system>login-control>telnet

config>system>login-control>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

5

Parameters

value

Specifies the maximum number of concurrent inbound Telnet sessions, expressed as an integer.

Values 0 to 7

login-banner

Syntax

[**no**] **login-banner**

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables or disables the display of a login banner. The login banner contains the 7210 SAS copyright and build date information for a console login attempt.

The **no** form of this command causes only the configured pre-login message and a generic login prompt to display.

login-control

Syntax

login-control

Context

config>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure the session control for the console, Telnet, and FTP.

motd

Syntax

motd {**url** *url-prefix***:** *source-url* | **text** *motd-text-string*}

no motd

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the message.

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*

Specifies 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

config>system>login-control>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

outbound-max-sessions 5

Parameters

value

Specifies the maximum number of concurrent outbound Telnet sessions, expressed as an integer.

Values 0 to 7

pre-login-message

Syntax

pre-login-message *login-text-string* [**name**]

no pre-login-message

Context

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command creates a message displayed before 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 this command removes the message.

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, and so on), the entire string must be enclosed within double quotes.

name

Keyword to always display the configured system name 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>security

config>system>login-control

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure the SSH parameters.

disable-graceful-shutdown

Syntax

[**no**] **disable-graceful-shutdown**

Context

config>system>login-control>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables graceful shutdown of SSH sessions.

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

client-cipher-list

Syntax

client-cipher-list protocol-version *version*

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the configuration of a list of allowed ciphers by the SSH client.

Parameters

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 that support SSH protocol version 2.

cipher

Syntax

cipher *index* **name** *cipher-name*

no cipher *index*

Context

config>system>security>ssh>client-cipher-list

config>system>security>ssh>server-cipher-list

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the configuration of a cipher. Client-ciphers are used when the 7210 SAS is acting as an SSH client. Server ciphers are used when the 7210 SAS is acting as an SSH server.

The **no** form of this command removes the index and cipher name from the configuration.

Default

no cipher *index*

Parameters

index

Specifies the index of the cipher in the list.

Values 1 to 255

cipher-name

Specifies the algorithm used when performing encryption or decryption.

Values The following table lists the default ciphers used for SSHv1.

Table 12: SSHv1 default ciphers

Cipher index value	Cipher name	Cipher	
		Client	Server
200	3des	✓	✓
205	blowfish	✓	✓
210	des	✓	

Values The following table lists the default ciphers used for SSHv2.

Table 13: SSHv2 default ciphers

Cipher index value	Cipher name	Cipher	
		Client	Server
190	aes256-ctr	✓	✓
192	aes192-ctr	✓	✓
194	aes128-ctr	✓	✓
200	aes128-cbc	✓	✓
205	3des-cbc	✓	✓
210	blowfish-cbc	✓	✓
215	cast128-cbc	✓	✓
220	arcfour	✓	✓
225	aes192-cbc	✓	✓
230	aes256-cbc	✓	✓

Cipher index value	Cipher name	Cipher	
		Client	Server
235	rijndael-cbc	✓	✓

client-mac-list

Syntax

client-mac-list

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure SSH MAC algorithms for the 7210 SAS acting as a client.

mac

Syntax

mac *index* **name** *mac-name*

no mac *index*

Context

config>system>security>ssh>client-mac-list

config>system>security>ssh>server-mac-list

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the user to configure SSH MAC algorithms for the 7210 SAS acting as an SSH server or an SSH client.

The **no** form of this command removes the specified **mac** index.

Default

no mac *index*

Parameters

index

Specifies the index of the algorithm in the list.

Values 1 to 255

mac-name

Specifies the algorithm for calculating the message authentication code.

Values The following table lists the default client and server algorithms used for SSHv2.

Table 14: SSHv2 default client and server algorithms

Cipher index value	MAC name
200	hmac-sha2-512
210	hmac-sha2-256
215	hmac-sha1
220	hmac-sha1-96
225	hmac-md5
230	hmac-ripemd160
235	hmac-ripemd160-openssh-com
240	hmac-md5-96

client-kex-list

Syntax

client-kex-list

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure SSH KEX algorithms for the 7210 SAS in the client role.

By default, the SSH advertises a KEX list that contains the following algorithms:

- diffie-hellman-group16-sha512

- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

kex

Syntax

kex *index* **name** *kex-name*

no kex *index*

Context

config>system>security>ssh>client-kex-list

config>system>security>ssh>server-kex-list

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures phase 1 SSHv2 KEX algorithms for the 7210 SAS in the SSH server or client role.

The **no** form of this command removes the specified KEX index. If all KEX indexes are removed, the default list is used.

Parameters

index

Specifies the index of the algorithm in the list. The lowest KEX index is negotiated first and the highest index, which is at the bottom of the KEX list, is negotiated last in the SSH negotiation.

Values 1 to 255

kex-name

Specifies the KEX algorithm for computing the shared secret key.

Values diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1

preserve-key

Syntax

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

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the server to save private keys, public keys, and host key files. It is restored following a system reboot or an SSH server restart.

The **no** form of this 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-cipher-list

Syntax

server-cipher-list protocol-version *version*

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the configuration of the list of allowed ciphers by the SSH server.

Parameters

version

Specifies the SSH version.

Values **1** — Specifies that the SSH server only accepts connections from clients that support SSH protocol version 1

2 — Specifies that the SSH server accepts connections from clients supporting either SSH protocol version 2

server-kex-list

Syntax

server-kex-list

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure SSH KEX algorithms for the 7210 SAS in the SSH server role.

By default, the SSH advertises a KEX list that contains the following algorithms:

- diffie-hellman-group16-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

server-mac-list

Syntax

server-mac-list

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the user to configure SSH MAC algorithms for the 7210 SAS acting as an SSH server.

server-shutdown

Syntax

[**no**] **server-shutdown**

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables the SSH servers running on the system. At system startup, only the SSH server is enabled.

version

Syntax

version *ssh-version*

no version

Context

config>system>security>ssh

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the SSH protocol version that will be supported by the SSH server.

Default

version 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure the Telnet login control parameters.

enable-graceful-shutdown

Syntax

[**no**] **enable-graceful-shutdown**

Context

config>system>login-control>telnet

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables graceful shutdown of Telnet sessions.

The **no** form of this command disables graceful shutdown of Telnet sessions.

2.9.2.1.3 Management Access Filter commands

management-access-filter

Syntax

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

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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 networks or subnetworks or through designated ports.

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

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

ip-filter

Syntax

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

Context

config>system>security>mgmt-access-filter

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure management access IP filter parameters.

ipv6-filter

Syntax

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

Context

config>system>security>mgmt-access-filter

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables 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.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures 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 this command removes the specified entry from the management access filter.

Parameters

entry-id

An entry ID uniquely identifies a match criteria and the corresponding action. Nokia recommends that entries be 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 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables 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.

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>entry

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a source TCP or UDP port number or port range for a management access filter match criterion.

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

Parameters

port

Specifies the source TCP or UDP port number as match criteria.

Values 1 to 65535 (decimal)

mask

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

This 16-bit mask can be configured using the formats listed in the following table.

Table 15: 16-bit mask configurations

Format style	Format syntax	Example
Decimal	DDDDD	63488

Format style	Format syntax	Example
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBBB	0b1111100000000000

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

Default 65535 (exact match)

Values 1 to 65535 (decimal)

fragment

Syntax

[**no**] **fragment** {**true** | **false**}

Context

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Note:
An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, and so on) fragments of a fragmented packet because only the first fragment contains the Layer 4 information.

The **no** form of this 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>entry

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a source TCP or UDP port number for an IP filter match criterion.

Note:
an entry containing L4 match criteria will not match non-initial (2nd, 3rd, and so on) fragments of a fragmented packet because only the first fragment contains the L4 information.

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

Default

no l4-src-port

Parameters

port

Specifies the source port number to be used as a match criteria expressed as a decimal integer.

Values 1 to 65535

mask

Specifies the mask in dotted-decimal notation

Values 1 to 65535 decimal hex or binary

flow-label

Syntax

flow-label *value*

no flow-label

Context

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Parameters

value

Specifies the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows, in accordance with RFC 3595, *Textual Conventions for IPv6 Flow Label*.

Values 0 to 1048575

log

Syntax

[**no**] **log**

Context

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

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Default

no log

next-header

Syntax

next-header *next-header*

no next-header

Context

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Parameters

next-header

Specifies the IP protocol field for IPv4 Management Access Filter (MAF), and the next header type to be used in the match criteria for this MAF entry for IPv6.

Values next-header: 0 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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 this command removes the protocol from the match criteria.

Parameters

protocol

Specifies the protocol number for the match criterion.

Values 1 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Default

base

Parameters

router-instance

Specifies the router name.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

The system exits on the first match found and executes the actions in accordance with the accompanying **action** command. This may require some entries to be renumbered differently from most to least explicit.

Parameters

old-entry-number

Specifies the entry number of the existing entry.

Values 1 to 9999

new-entry-number

Specifies the new entry number that will replace the old entry number.

Values 1 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command restricts ingress management traffic to either the CPM Ethernet port or any other logical port (LAG or port) on the device.

When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria.

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

Default

any interface

Parameters

port-id

Specifies 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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 this command removes the source IP address match criterion.

Parameters

ip-prefix/prefix-length

Specifies the IP prefix used for IP match criteria in dotted-decimal notation. It can be IPv4 or an IPv6 prefix.

Values ipv4-prefix: a.b.c.d

ipv4-prefix-length: 0 to 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 to 128

netmask

Specifies the subnet mask in dotted-decimal notation.

Values a.b.c.d (network bits all 1 and host bits all 0)

2.9.2.1.4 Distributed CPU protection commands

dist-cpu-protection

Syntax

dist-cpu-protection

Context

config>system>security

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

Commands in this context configure distributed CPU protection.

policy

Syntax

policy *policy-name* [**create**]

no policy *policy-name*

Context

config>sys>security>dist-cpu-protection

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command configures one of the maximum 16 distributed CPU protection policies. These policies can be applied to objects such as SAPs.

Parameters

policy-name

Specifies the policy name, up to 32 characters.

create

Creates a new policy instance.

description

Syntax

description *description-string*

no description

Context

config>system>security>dist-cpu-protection>policy

config>system>security>dist-cpu-protection>policy>static-policer

Platforms

7210 SAS-R6 and 7210 SAS-R12

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 this command removes the string.

Default

no description

Parameters

string

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

protocol

Syntax

protocol *name* [**create**]

no protocol *name*

Context

config>sys>security>dist-cpu-protection>policy

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command creates the protocol for control in the policy.

For RVPLS, DCP rate-limits the packets arriving at the CPU, but for flooded traffic, ingress QoS or ACLs must be used.

When the **no** form of this command is used, the packets of the specified protocol are not enforced on the objects to which this DCP policy is assigned.

Parameters

names

Specifies the protocol name.

Values arp, icmp, igmp, vrrp, ntp

create

Creates a new protocol instance.

enforcement

Syntax

enforcement {**static** *policer-name*}

Context

config>sys>security>dist-cpu-protection>policy>protocol

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command configures the enforcement method for the protocol. When the **static** keyword is used, the protocol is always enforced using a static policer. Multiple protocols can reference the same static policer. When multiple protocols are configured to reference the same policer, each protocol is assigned an independent instance of the policer. The policer is not shared among the multiple protocols that are referencing it.

Default

enforcement dynamic local-mon-bypass

Parameters

static

Specifies that the protocol is always enforced using a static policer.

policer-name

Specifies the name of the static policer, up to 32 characters.

static-policer

Syntax

static-policer *policer-name* [**create**]

static-policer *policer-name*

Context

config>sys>security>dist-cpu-protection>policy

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command configures a static enforcement policer that can be referenced by one or more protocols in the policy. When the policer name is referenced by a protocol, this policer is instantiated for each protocol and each object (for example, SAP) that is created and references this policy. If there is no policer resource available, the object is blocked from being created. Multiple protocols can use the same static policer. When multiple protocols reference the same policer, each protocol gets an independent instance of the policer. The policer is not shared among the multiple protocols that are referencing it.

Parameters

policer-name

Specifies the name of the policer, up to 32 characters.

create

Keyword to create a new static-policer instance.

exceed-action

Syntax

exceed-action {**discard** | **none**}

Context

config>sys>security>dist-cpu-protection>policy>static-policer

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.

Default

exceed-action none

Parameters

discard

Keyword to discards packets that are non-conformant.

none

Keyword to send packets to the CPU instead of discarding them.

log-events

Syntax

log-events [**verbose**]

no log-events

Context

config>sys>security>dist-cpu-protection>policy>static-policer

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command controls the creation of log events related to static policer status and activity.

Default

log-events

Parameters

verbose

Keyword to send the same events as just log events. The optional keyword **verbose** includes events used during debugging, tuning, and investigation.

rate

Syntax

rate {**kbps** *kilobits-per-second* | **max**} {[**mbs** *size*] [**bytes** | **kilobytes**]}

no rate

Context

config>sys>security>dist-cpu-protection>policy>static-policer

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.

The hardware may not be able to rate limit to the exact configured parameters. In this case, the configured parameters are adapted to the closest supported rate. The actual (operational) parameters can be seen in CLI, for example, `show service id 33 sap 1/1/3:33 dist-cpu-protection detail`.

Default

rate kbps max mbs default

Parameters

kilobits-per-second

Specifies the kilobits per second.

Values 1 to 204800 | max (the max keyword disables the policer (always conformant))

size

Specifies the tolerance for the kbps rate.

Values *size-in-bytes*: [512 to 65536]

size-in-kbytes: [1 to 64]

bytes | kilobytes

Specifies that the units of the **mbs** *size* parameter are either in bytes or kilobytes.

2.9.2.1.5 Password commands

admin-password

Syntax

admin-password *password* [**hash** | **hash2**]

no admin-password

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables the context (with administrative permissions) to configure a password that 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 administrative 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 command. If the **admin-password** command is configured in the **config>system>security>password** context, any user can enter the special administrative mode by entering the **enable-admin** command.

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

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

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for this password are determined by the configuration in the **complexity-rules** context.

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

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 '****'.

Note:
The **configure system security password hashing** command affects the maximum number of characters that can be used to configure the *password* parameter.

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

Default

no admin-password

Parameters

password

Specifies the password, which enables a user to become a system administrator. The maximum length can be up to 56 characters if unhashed, 32 characters if the **hash** keyword is specified, and 54 characters if the **hash2** keyword is specified, 60 characters if hashed with **bcrypt**, or 87 to 92 characters if hashed with **sha2-pbkdf2**.

hash

Specifies that the key is entered in an encrypted form. If the **hash** keyword is not configured, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form.

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>

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

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

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

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

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

Output

The following output shows an example of an error message when the **enable-admin** command is entered at the prompt again and the user is already in the **enable-admin** mode.

Sample output

```
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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Parameters

days

Specifies the maximum number of days the password is valid.

Values 1 to 500

attempts

Syntax

attempts *count* [**time** *minutes1* [**lockout** *minutes2*]

no attempts

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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*. An SNMP trap is generated by the device when the number of login attempts exceeds the configured threshold. Generation of the trap can be suppressed 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. An 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** form of this command reverts to the default values.

Default

attempts 3 time 5 lockout 10

Parameters

count

Specifies the number of unsuccessful login attempts allowed for the specified **time**. This is a mandatory value that must be explicitly entered.

Values 1 to 64

Default 3

time *minutes*

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

Values 0 to 60

Default 5

lockout *minutes*

Specifies the lockout period, in minutes, where the user is not allowed to login. Allowed values are decimal integers.

Values 0 to 1440

Default 10

authentication-order

Syntax

authentication-order [*method-1*] [*method-2*] [*method-3*] [**exit-on-reject**]

no authentication-order

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, an entry in the security log registers the failed attempt. The attempted login identification and originating IP address are logged with the a timestamp.

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

Default

authentication-order radius tacplus local

Parameters

method-1

Specifies the first password authentication method to attempt.

Values radius, tacplus, local

Default radius

method-2

Specifies the second password authentication method to attempt.

Values radius, tacplus, local

Default tacplus

method-3

Specifies the third password authentication method to attempt.

Values radius, tacplus, local

Default local

radius

Specifies the RADIUS authentication.

tacplus

Specifies the TACACS+ authentication.

local

Specifies the 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, the next method in the order will not be tried. If the **exit-on-reject** keyword is not specified and 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.

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, **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.

If the user is configured locally but without console access, login will be denied.

complexity-rules

Syntax

complexity-rules

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context define a list of rules for configurable password options.

allow-user-name

Syntax

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

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables the username to be used as part of the password.

The **no** form of this command does not allow the username to be used as part of the password.

credits

Syntax

credits [**lowercase** *credits*] [**uppercase** *credits*] [**numeric** *credits*] [**special-character** *credits*]

no credits

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Default

no credits

Parameters

credits

Specifies the number of credits that can be used for each characters class.

Values 0 to 10

minimum-classes

Syntax

minimum-classes *minimum*

no minimum-classes

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command forces the use of at least the specified number of different character classes.

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

Default

no minimum-classes

Parameters

minmum

Specifies the minimum number of classes to be configured.

Values 2 to 4

health-check

Syntax

[**no**] **health-check** [**interval** *interval*]

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies that RADIUS, TACACS+, and LDAP 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, a trap will be sent based on the server type.

The **no** form of this command disables the periodic monitoring of the RADIUS, TACACS+, and LDAP servers. In this case, the operational status for the active server will be up if the last access was successful.

Parameters

interval

Specifies the polling interval for RADIUS, TACACS+, and LDAP servers.

Values 6 to 1500

Default 30

history

Syntax

history *size*

no history

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures how many previous passwords a new password is matched against.

Default

no history

Parameters

size

Specifies how many previous passwords a new password is matched against.

Values 1 to 20

minimum-age

Syntax

minimum-age [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]

no minimum-age

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the minimum required age of a password before it can be changed again.

The **no** form of this command removes the minimum password age requirement.

Default

no minimum-age

Parameters

days

Specifies the minimum number of days before a password can be changed again.

Values 0 to 1

hours

Specifies the minimum number of hours before a password can be changed again.

Values 0 to 23

minutes

Specifies the minimum number of minutes before a password can be changed again.

Values 0 to 59

seconds

Specifies the minimum number of seconds before a password can be changed again.

Values 0 to 59

minimum-change

Syntax

minimum-change *length*

no minimum-change

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the minimum number of characters required to be different in the new password from a previous password.

The **no** form of this command removes the unique character requirement.

Default

no min-change

Parameters

length

Specifies how many characters must be different in the new password from the old password.

Values 2 to 20

minimum-length

Syntax

minimum-length *length*

no minimum-length

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the minimum number of characters required for locally administered passwords and keys used with SNMPv3 user authentication and encryption. See the **configure system security user snmp** authentication command for more information about the use of keys with SNMPv3-based authentication and encryption algorithms.

If multiple **minimum-length** commands are entered, each new command overwrites the previously configured password length.

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

Default

minimum-length 6

Parameters

value

Specifies the minimum number of characters required for a locally administered password.

Values 6 to 50

repeated-characters

Syntax

repeated-characters *count*

no repeated-characters

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the number of times a character can be repeated consecutively.

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

Default

no repeated-characters

Parameters

count

Specifies the minimum count of consecutively repeated characters.

Values 2 to 8

required

Syntax

required [**lowercase** *count*] [**uppercase** *count*] [**numeric** *count*] [**special-character** *count*]

no required

Context

config>system>security>password>complexity-rules

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the minimum number of different character classes required.

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

Default

no required

Parameters

count

Specifies the minimum count of characters classes.

Values 0 to 10

hashing

Syntax

hashing {**bcrypt** | **sha2-pbkdf2**}

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the password hashing algorithm.

Parameters

bcrypt

Keyword to configure the bcrypt algorithm.

sha2-pbkdf2

Keyword to configure the PBKDF2 algorithm.

health-check

Syntax

[**no**] **health-check** [**interval** *interval*]

Context

config>system>security>password

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, a trap will be sent based on the type of the server.

The **no** form of this 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 to 1500

password

Syntax

password

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure password management parameters.

public-keys

Syntax

public-keys

Context

config>system>security>user

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure public keys for SSH.

ecdsa

Syntax

ecdsa

Context

config>system>security>user>public-keys

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ECDSA public keys.

ecdsa-key

Syntax

ecdsa-key *ecdsa-public-key-id* [**create**]

no ecdsa-key *ecdsa-public-key-id*

Context

config>system>security>user>public-keys>ecdsa

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates an ECDSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

The **no** form of this command removes the configured ECDSA public keys.

Default

no ecdsa-key

Parameters

create

Keyword to create an ECDSA key. The **create** keyword requirement can be enabled or disabled in the **environment**>**create** context.

key-id

Specifies the key identifier.

Values 1 to 32

key-value

Syntax

key-value *public-key-value*

no key-value

Context

config>system>security>user>public-keys>ecdsa>ecdsa-key

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a value for the ECDSA public key. The public key must be enclosed in quotation marks. The key is between 1 and 1024 bits.

The **no** form of this command removes the configured ECDSA public key value.

Default

no key-value

Parameters

ecdsa-public-key-value

Specifies the public key value, up to 255 characters.

rsa

Syntax

rsa

Context

config>system>security>user>public-keys

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure RSA public keys.

rsa-key

Syntax

rsa-key *rsa-public-key-id* [**create**]

no rsa-key *rsa-public-key-id*

Context

config>system>security>user>public-keys>rsa

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates an RSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

The **no** form of this command removes the configured RSA public keys.

Default

no rsa-key

Parameters

create

Keyword to create the RSA key. The **create** keyword requirement can be enabled or disabled in the **environment**>**create** context.

key-id

Specifies the key identifier.

Values 1 to 32

key-value

Syntax

key-value *rsa-public-key-value*

no key-value

Context

config>system>security>user>public-keys>rsa>rsa-key

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a value for the RSA public key. The public key must be enclosed in quotation marks. The key is between 768 and 4096 bits.

The **no** form of this command removes the configured public key value.

Default

no key-value

Parameters

public-key-value

Specifies the public key value, up to 800 characters.

2.9.2.1.6 Profile management commands

action

Syntax

action {**deny** | **permit**}

Context

config>system>security>profile>entry

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the action associated with the profile entry.

Parameters

deny

Specifies that commands matching the entry command match criteria are denied.

permit

Specifies that commands matching the entry command match criteria are permitted.

match

Syntax

match *command-string*

no match

Context

config>system>security>profile>entry

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a command or command subtree.

Because the system 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 before this profile.

All commands below the hierarchy level of the matched command are denied.

The **no** form of this command removes a match condition.

Parameters

command-string

Specifies 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Parameters

source-user

Specifies the user, up to 32 characters, to copy from. The user must already exist.

source-profile

Specifies the profile, up to 32 characters, to copy from. The profile must already exist.

destination

Specifies the destination profile, up to 32 characters, to which the profile is copied.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the default action to be applied when no match conditions are met.

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:
The **permit-all** keyword 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**, 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, the second profile will be evaluated. If the default action of the last profile is **none** and no explicit match is found, the default **deny-all** takes effect.

description

Syntax

description *description-string*

no description

Context

config>system>security>profile>entry

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the string from the context.

Parameters

description-string

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

entry

Syntax

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

Context

config>system>security>profile

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command is used to create a user profile entry.

More than one entry can be created with unique *entry-id* numbers. The 7210 SAS 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 this command removes the specified entry from the user profile.

Parameters

entry-id

Specifies the 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 to 9999

profile

Syntax

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

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command creates 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.

When 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 this command deletes a user profile.

Default

user-profile default

Parameters

user-profile-name

Specifies 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command renumbers profile entries to resequence the entries.

Because the 7210 SAS exits when the first match is found and executes the actions according to the accompanying **action** command, renumbering is useful to rearrange the entries from most explicit to least explicit.

Parameters

old-entry-number

Specifies the entry number of an existing entry.

Values 1 to 9999

new-entry-number

Specifies the new entry number.

Values 1 to 9999

2.9.2.1.7 User management commands

access

Syntax

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

Context

config>system>security>user

config>system>security>user-template

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

If a user requires access to more than one application, multiple applications can be specified in a single command. Multiple commands are treated additively.

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

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

authentication *authentication-protocol key-1* [**privacy none**] [**hash** | **hash2**]

authentication *authentication-protocol key-1* **privacy** *privacy-protocol key-2* [**hash | hash2**]

no authentication

Context

config>system>security>user>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the authentication and encryption method that the device uses to validate the user. The SNMP authentication allows the device to validate the managing node that issues the SNMP message and detect message tampering.

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

Default

authentication none

Parameters

authentication-protocol

Specifies the SNMP authentication protocol.

Values **hmac-md5-96** — Specifies the use of the HMAC-MD5-96 authentication protocol.

hmac-sha1-96 — Specifies the use of the HMAC-SHA-96 authentication protocol.

hmac-sha2-224 — Specifies the use of the HMAC-SHA-224 authentication protocol.

hmac-sha2-256 — Specifies the use of the HMAC-SHA-256 authentication protocol.

hmac-sha2-384 — Specifies the use of the HMAC-SHA-384 authentication protocol.

hmac-sha-512 — Specifies the use of the HMAC-SHA-512 authentication protocol.

privacy-protocol

Specifies the SNMP privacy protocol.

Values **none** — Specifies that encryption should not be used.

cbc-des — Specifies the use of the CBC-DES privacy protocol.

cfb128-aes-128 — Specifies the use of the CFB128-AES-128 privacy protocol.

cfb128-aes-192 — Specifies the use of the CFB128-AES-192 privacy protocol.

cfb128-aes-256 — Specifies the use of the CFB128-AES-256 privacy protocol.

hash

Keyword to indicate the encryption mechanism used to store the authentication and privacy keys in an encrypted format in the configuration file. When **hash** is not specified, non-encrypted characters can be entered. When hash is specified, the key is expected to be decrypted using the hash mechanism. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** keyword specified.

hash2

Keyword to indicate the encryption mechanism used to store all specified keys in an encrypted format in the configuration file. For example, the **hash2** encrypted variable cannot be copied and pasted to a different node. If the **hash2** keyword is not specified, the key is assumed to be unencrypted in cleartext form. The **hash2** keyword is the default mechanism used if hash is not specified. Therefore, the user does not need to specify **hash2** explicitly while entering the key. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** keyword specified.

key-1

Specifies the *key-1* value for SNMP packet encryption.

Values **localized-privacy-key** — Key value generated by using the **tools>perform>system>management-interface>snmp>generate-key** command. When this key is stored in the configuration, it is stored in encrypted form using one of the mechanisms available (for example, hash or hash2) along with the keyword to indicate the mechanism used (for example, **config>system>security>user** *"User1"* **snmp>privacy cbc-des** *e8482d1f66e057450afa6e* **hash**).

hash-key — Key value obtained by using the hash mechanism to store the key in encrypted format in the configuration

file. Initially the key value is generated by using the **tools>perform>system>management-interface>snmp>generate-key** command and further stored in the configuration using the hash mechanism.

hash2-key — Key value obtained by using the hash2 mechanism for encrypting the key. This value cannot be entered by the user. It is automatically generated using the hash2 mechanism, when the user does not explicitly specify the hash mechanism for encrypting the key, and stored in the configuration file.

key-2

Specifies the *key-2* value for SNMP packet encryption.

Values **localized-privacy-key** — Key value generated by using the **tools>perform>system>management-interface>snmp>generate-key** command. When this key is stored in the configuration, it is stored in encrypted form using one of the mechanisms available (for example, hash or hash2) along with the keyword to indicate the mechanism used (for example, **config>system>security>user** *"User1"* **snmp>authentication hmac-md5-96** *e8482d1f66e057a0be0e50afa6e* **hash**).

hash-key — Key value obtained by using the hash mechanism to store the key in encrypted format in the configuration file. Initially, the key value is generated by using the **tools>perform>system>management-interface>snmp>generate-key** command and further stored in the configuration using the hash mechanism.

hash2-key — Key value obtained by using the **hash2** mechanism for encrypting the key. This value cannot be entered by the user. It is automatically generated using the hash2 mechanism, when the user does not explicitly specify the hash mechanism for encrypting the key, and stored in the configuration file.

group

Syntax

group *group-name*

no group

Context

config>system>security>user>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 models, security levels, and read, write, and notify permissions

Parameters

group-name

Specifies the group name, up to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command allows a user to change their password for FTP and console login.

To disable a user password change privilege, use the **cannot-change-password** form of this command.

Note:
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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command copies a specific user configuration parameter to another (destination) user.

The password is set to a carriage return and a new password at login must be selected.

Parameters

source-user

Specifies the user, up to 32 characters, to copy. The user must already exist.

destination

Specifies the destination user or profile, up to 32 characters.

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*] [*directoryIdirectory…*]

no home-directory

Context

config>system>security>user

config>system>security>user-template

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, a warning message is issued and the default is assumed.

The **no** form of this command removes the configured home directory.

Note:
If **restricted-to-home** has been configured, no file access is granted and no home directory is created. If **restricted-to-home** is not applied, the root becomes the user home directory.

Default

no home-directory

Parameters

local-url-prefix [directory] [directory/directory…]

Specifies the user local home directory URL prefix and directory structure, up to 190 characters.

profile

Syntax

profile *user-profile-name*

no profile

Context

config>system>security>user-template

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Parameters

user-profile-name

Specifies 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a user 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 this command disables the login exec file for the user.

Parameters

url-prefix*:*source-url

Specifies either a local or remote URL, up to 200 characters, 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command gives the user access to a profile.

A user can participate in up to eight profiles.

The **no** form of this command deletes user access to a profile.

Default

default

Parameters

user-profile-name

Specifies the user profile name, up to 32 characters.

new-password-at-login

Syntax

[**no**] **new-password-at-login**

Context

config>system>security>user>console

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 specific 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 specific password is already hashed using hashing algorithm version 2. A semantic check is performed on the specific 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 is up to 20 characters if unhashed, 32 characters if hashed.

All password special characters (#, $, spaces, and so on) 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 ? character, enter them inside a notepad or clipboard program, and cut and pasted them 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 specific password is already hashed using hashing algorithm version 1. A semantic check is performed on the specific password field to verify if it is a valid hash 1 key to store in the database.

hash2

Specifies that the specific password is already hashed using hashing algorithm version 2. A semantic check is performed on the specific 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, the user has no file access.

The **no** form of this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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.

The 7210 SAS always uses the configured SNMPv3 username as the security username.

user-template

Syntax

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

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the context to edit the user configuration.

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

user

Syntax

user *user-name*

Context

admin

config>system>security>user

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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 entering the **info** command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that username, there will be no password required. The user can login to the system and <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 this command deletes the user and all configuration data. Users cannot delete themselves.

Parameters

user-name

Specifies the name of the user, up to 16 characters.

2.9.2.1.8 RADIUS client commands

accounting

Syntax

[**no**] **accounting**

Context

config>system>security>radius

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.

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

Parameters

port

Specifies the UDP port number.

Values 1 to 65535

Default 1813

authorization

Syntax

[**no**] **authorization**

Context

config>system>security>radius

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures RADIUS authorization parameters for the system.

Default

no authorization

port

Syntax

port *port*

no port

Context

config>system>security>radius

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the TCP port number to contact the RADIUS server.

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

Default

port 1812

Parameters

port

The TCP port number to contact the RADIUS server.

Values 1 to 65535

radius

Syntax

[**no**] **radius**

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure RADIUS authentication on the router.

Implement redundancy by configuring multiple server addresses for each router.

The **no** form of this command removes the RADIUS configuration.

retry

Syntax

retry *count*

no retry

Context

config>system>security>radius

config>system>security>dot1x>radius-plcy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

retry 3

Parameters

count

Specifies the retry count.

Values 1 to 10

server

Syntax

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a RADIUS server and its 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 this command removes the server from the configuration.

Parameters

index

Specifies 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 to 5

address ***ip-address***

Specifies 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***

Specifies the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values 20 characters maximum

hash

Specifies that the key is entered in an encrypted form. If the **hash** keyword 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 that 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Default

no shutdown

timeout

Syntax

timeout *seconds*

no timeout

Context

config>system>security>radius

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Default

3 seconds

Parameters

seconds

Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

use-default-template

Syntax

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

Context

config>system>security>radius

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command disables the command.

2.9.2.1.9 TACACS+ client commands

server

Syntax

server *index* **address** *ip-address* **secret** *key* [**hash** | **hash2**] [**port** *port*]

no server *index*

Context

config>system>security>tacplus

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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 this command removes the server from the configuration.

Parameters

index

Specifies 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 to 5

address *ip-address*

Specifies 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*

Specifies the secret key to access the RADIUS server, up to 128 characters. This secret key must match the password on the RADIUS server.

hash

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

hash2

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

tacplus

Syntax

[**no**] **tacplus**

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the TACACS+ configuration.

accounting

Syntax

accounting [**record-type** {**start-stop** | **stop-only**}]

no accounting

Context

config>system>security>tacplus

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the type of accounting record packet 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures TACACS+ authorization parameters for the system.

Default

no authorization

timeout

Syntax

timeout *seconds*

no timeout

Context

config>system>security>tacplus

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Default

timeout 3

Parameters

seconds

Specifies the number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 to 90

shutdown

Syntax

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

Context

config>system>security>tacplus

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

2.9.2.1.10 Generic 802.1x commands

dot1x

Syntax

[**no**] **dot1x**

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command creates the context to configure 802.1x network access control on the 7210 SAS.

The **no** form of this command removes the 802.1x configuration.

radius-plcy

Syntax

[**no**] **radius-plcy** *name* [**create**]

Context

config>system>security> dot1x

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure RADIUS server parameters for 802.1x network access control on the 7210 SAS.

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 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.

The **no** form of this command removes the RADIUS server configuration for 802.1x.

Parameters

name

Specifies the name of the RADIUS policy, up to 32 characters.

create

This keyword is mandatory to create a RADIUS policy.

retry

Syntax

retry *count*

no retry

Context

config>system>security> dot1x

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to the default value.

Default

retry 3

Parameters

count

Specifies the retry count.

Values 1 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

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

Parameters

server-index

Specifies 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 to 5

address *ip-address*

Specifies 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*

Specifies the secret key to access the Dot1x server. This secret key must match the password on the Dot1x server.

Values secret-key - 20 characters maximum

Values hash-key - 33 characters maximum

Values hash2-key - 55 characters maximum

hash

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

hash2

Specifies that 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***

Specifies the UDP port number on which to contact the RADIUS server for accounting requests.

Values 1 to 65535

auth-port ***auth-port***

Specifies a UDP port number to be used as a match criteria.

Values 1 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the NAS IP address to be sent in the RADIUS packet.

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

Default

By default the system IP address is used in the NAS field.

Parameters

ip-address

Specifies the IP prefix for the IP match criterion in dotted-decimal notation.

Values a.b.c.d

shutdown

Syntax

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

Context

config>system>security>dot1x

config>system>security>dot1x>radius-plcy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Default

timeout 3

Parameters

seconds

Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

2.9.2.1.11 TCP Enhanced Authentication commands

keychain

Syntax

[**no**] **keychain** *keychain-name*

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

The **no** form of this 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.

Parameters

keychain-name

Specifies a keychain name, up to 32 characters, which identifies this particular keychain entry.

direction

Syntax

direction

Context

config>system>security>keychain

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the context to specify the data type that indicates the TCP stream direction to apply the keychain.

bi

Syntax

bi

Context

config>system>security>keychain>direction

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures keys for both send and receive stream directions.

uni

Syntax

uni

Context

config>system>security>keychain>direction

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures keys for send or receive stream directions.

receive

Syntax

receive

Context

config>system>security>keychain>direction>uni

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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.

send

Syntax

send

Context

config>system>security>keychain>direction>uni

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the entry from the keychain. If the entry is the active entry for sending, 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, the system will reject the command with an error indicating that 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, the command will not be accepted, and an error message indicating that this is the only eligible key will be generated.

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

Parameters

entry-id

Specifies an entry that represents a key configuration to be applied to a keychain.

Values 0 to 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

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

hash2

Specifies that 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and 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]

UTC

Specifies that the date and time should be in UTC time rather than local time.

now

Specifies that 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, in seconds.

Values 0 to 4294967294

forever

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

tcp-option-number

Syntax

tcp-option-number

Context

config>system>security>keychain

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Default

receive 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 and 254

send

Syntax

send *option-number*

Context

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Default

send 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

The **no** form of this 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 to 65535 (accepted in decimal hex or binary)

mask

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

lockout

Syntax

lockout all

lockout user *user-name*

Context

admin>clear

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command is used to clear a lockout for a specific user.

Parameters

user-name

Specifies the locked user name, up to 32 characters.

all

Clears lockouts for all users.

2.9.2.1.12 IPsec commands

ipsec

Syntax

ipsec

Context

config

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

Commands in this context configure Internet Protocol security (IPsec) parameters. IPsec is a structure of open standards that uses cryptographic security services to ensure private, secure communications over IP networks.

static-sa

Syntax

static-sa *sa-name* [**create**]

no static-sa

Context

config>ipsec

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command configures an IPsec static security association (SA).

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

Parameters

sa-name

Specifies the SA name, up to 32 characters.

create

Mandatory keyword to create an SA instance.

authentication

Syntax

authentication *auth-algorithm* **ascii-key** *ascii-string*

authentication *auth-algorithm* **hex-key** *hex-string* [**hash** | **hash2**]

no authentication

Context

config>ipsec>static-sa

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command configures the authentication algorithm to use for an IPsec manual SA.

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

Default

no authentication

Parameters

auth-algorithm

Specifies the authentication algorithm.

Values **sha1** — The authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96.

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

ascii-string

Specifies the ASCII key, up to 16 characters for **md5** and 20 characters for **sha1**.

The authentication key is stored an encrypted format. The minimum key length is configured using the **config>system>security>password>minimum-length** command.

The complexity of the key is configured using the commands in the **config>system>security>password>complexity-rules** context.

hex-string

Specifies the hexadecimal key, up to 32 hexadecimal nibbles for **md5** and up to 40 hexadecimal nibbles for **sha1**.

hash

Keyword that stores all specified keys in encrypted format in the configuration file. The password must be entered in encrypted form when this keyword is configured. If this keyword is not configured, the key is assumed to be in a non-encrypted form.

hash2

Keyword to store the key in a more complex encrypted form. If this keyword is not used, the less encrypted **hash** form is assumed.

description

Syntax

description *description-string*

no description

Context

config>ipsec>static-sa

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command creates a text description, which is stored in the configuration file, to help identify the content of the entity.

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

Parameters

description-string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. It the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed in double quotes.

direction

Syntax

direction *ipsec-direction*

no direction

Context

config>ipsec>static-sa

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command configures the direction for an IPsec manual SA.

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

Default

direction bidirectional

Parameters

ipsec-direction

Specifies the direction.

Values inbound, outbound, bidirectional

protocol

Syntax

protocol *ipsec-protocol*

no protocol

Context

config>ipsec>static-sa

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command configures the security protocol to use for an IPsec manual SA.

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

Default

protocol esp

Parameters

ipsec-protocol

Specifies the security protocol.

Values **ah** — Configures to Authentication Header Protocol.

esp — Configures the Encapsulation Security Payload Protocol.

spi

Syntax

spi *spi*

no spi

Context

config>ipsec>static-sa

Platforms

Supported on all 7210 SAS platforms as described in this document, except those operating in access-uplink mode

Description

This command configures the security parameter index (SPI) key value for an IPsec manual SA.

The **no** form of this command removes the configured SPI key value.

Parameters

spi

Specifies the SPI value.

Values 256 to 16383

2.9.2.2 Show commands

- Security commands
- Login control

2.9.2.2.1 Security commands

access-group

Syntax

access-group [*group-name*]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays SNMP access group information.

Parameters

group-name

Displays information for the specified access group name, up to 32 characters.

Output

The following output is an example of SNMP access group information, and Table 16: Output fields: access group describes the output fields.

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#
```

Table 16: Output fields: access group

Label	Description
Group name	Displays the access group name
Security model	Displays 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

authentication

Syntax

authentication [**statistics**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays system login authentication configuration and statistics.

Parameters

statistics

Appends login and accounting statistics to the display.

Output

The following output is an example of system login authentication information, and Table 17: Output fields: security authentication describes the output fields.

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#
```

Table 17: Output fields: security authentication

Label	Description
Sequence	Displays the sequence in which authentication is processed
Server address	Displays the IP address of the RADIUS server
Status	Displays the current status of the RADIUS server
Type	Displays the authentication type
Timeout (secs)	Displays 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	Displays the number of times the user has successfully logged in
Rejected logins	Displays the number of unsuccessful login attempts
Sent packets	Displays the number of packets sent
Rejected packets	Displays the number of packets rejected

dist-cpu-protection

Syntax

cpu-protection

Context

show>system>security

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

Commands in this context display distributed CPU protection information.

policy

Syntax

policy [*name*] [**association** | **detail**]

Context

show>system>security>dist-cpu-protection

Platforms

7210 SAS-R6 and 7210 SAS-R12

Description

This command displays distributed CPU protection policy information.

Parameters

name

Displays distributed CPU protection policy information for the specified policy name, up to 32 characters.

association

Displays associations for the specified policy name.

detail

Displays detailed information for the specified policy name.

keychain

Syntax

keychain [*key-chain*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays keychain information.

Parameters

key-chain

Specifies the keychain name to display.

detail

Displays detailed keychain information.

Output

The following output is an example of keychain information, and Table 18: Output fields: keychain describes the output fields.

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#
```

Table 18: Output fields: keychain

Label	Description
TCP-Option number send	Displays the TCP option number to be inserted in the header of sent TCP packets
Admin state	Displays the administrative state of the keychain: up or down

Label	Description
TCP-Option number receive	Displays the TCP option number that will be accepted in the header of received TCP packets
Oper state	Displays the operational state of the keychain: up or down
Key entries for key chain: *test*	
Id	Displays the ID of the key entry
Direction	Displays the stream direction on which keys will be applied for this entry: send, receive, or send-receive
Algorithm	Displays the encryption algorithm to be used by this key entry
Option	Indicates the configured IS-IS encoding standard (indicates "none" if the associated protocol is not IS-IS)
Admin State	Displays the administrative state of the key entry: up or down
Valid	Indicates if the receive key is valid
Active	Indicates if the transmit (sent) key is active
Tolerance	Displays the tolerance time configured for support of both currently active and new keys
Begin Time	Displays the time at which the new key is used to sign and/or authenticate protocol packets
Begin Time (UTC)	Displays the begin time in UTC time
End Time	Displays the time at which the key is no longer eligible to authenticate protocol packets
End Time (UTC)	Displays the end time in UTC time

management-access-filter

Syntax

management-access-filter

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays management access IP filters.

Parameters

entry-id

Displays information for the specified entry.

Values 1 to 9999

Output

The following output is an example of management access IP filter information, and Table 19: Output fields: IP filter describes the output fields.

Sample 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#
```

Table 19: Output fields: IP filter

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	Displays the entry ID in a policy or filter table
Description	Displays a text string describing the filter
Src IP	Displays the source IP address used for management access filter match criteria
Src Interface	Displays the interface name for the next-hop to which the packet should be forwarded if it hits this filter entry
Dest port	Displays the destination port
Match	Displays the number of times a management packet has matched this filter entry
Protocol	Displays the IP protocol to match
Action	Displays the action to take for packets that match this filter entry
Flow label	Displays the flow label value to match
Next-header	Displays the IPv6 next header value to match
L4 Src port	Displays the TCP/UDP source port number to match
Fragment	Indicates if the entry should match a fragment or not
Router	Displays the router Instance ID to match
Log	Indicates if packet matching this entry must be logged or not On 7210 SAS platforms, logging is not supported

ipv6-filter

Syntax

ipv6-filter [**entry** *entry-id*]

Context

show>system>security>mgmt-access-filter

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays management access IPv6 filters.

Parameters

entry-id

Displays information for the specified entry.

Values 1 to 9999

Output

The following output is an example of management access IPv6 filter information, and Table 20: Output fields: IPv6 filter describes the output fields.

Sample output

```
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#
```

Table 20: Output fields: IPv6 filter

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	Displays the entry ID in a policy or filter table
Description	Displays a text string describing the filter
Src IP	Displays the source IPv6 address used for management access filter match criteria
Src Interface	Displays the interface name for the next-hop to which the packet should be forwarded if it hits this filter entry
Dest port	Displays the destination port
Flow label	Displays the flow label value to match
Protocol	Displays the IPv6 protocol to match
Action	Displays the action to take for packets that match this filter entry
Next-header	Displays the IPv6 next header value to match
L4 Src port	Displays the TCP/UDP source port number to match
Router	Displays the router Instance ID to match
Log	Indicates if packet matching this entry must be logged or not On 7210 SAS platforms, logging is not supported

password-options

Syntax

password-options

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays configured password options.

Output

The following output is an example of password option information, and Table 21: Output fields: password options describes the output fields.

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#
```

Table 21: Output fields: password options

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

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

profile

Syntax

profile [*user-profile-name*]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays user profile information.

If the *user-profile-name* is not specified, information for all profiles are displayed.

Parameters

user-profile-name

Displays information for the specified user profile name, up to 32 characters.

Output

The following output is an example of user profile information, and Table 22: Output fields: profile describes the output fields.

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#
```

Table 22: Output fields: profile

Label	Description
User Profile	Displays the profile name used to deny or permit user console access to a hierarchical branch or to specific commands
Def. action	Permit all — Permits access to all commands Deny — Denies access to all commands None — No action is taken
Entry	Displays 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	Displays the total number of profiles listed

source-address

Syntax

source-address

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays source addresses configured for applications.

Output

The following output is an example of source address information, and Table 23: Output fields: source access describes the output fields.

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#
```

Table 23: Output fields: source access

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

ssh

Syntax

ssh

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays all the SSH sessions as well as the SSH status and fingerprint.

Output

The following output is an example of SSH session information, and Table 24: Output fields: SSH describes the output fields.

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#
```

Table 24: Output fields: SSH

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 identity Clients trying to connect to the server verify the server fingerprint If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed
Connection	Displays the IP address of the connected routers (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	Displays the name of the user

Label	Description
Number of SSH sessions	Displays the total number of SSH sessions

user

Syntax

user [*user-name*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays user registration information.

If no command line options are specified, summary information for all users is displayed.

Parameters

user-name

Displays information for the specified user name, up to 32 characters.

Default all users

detail

Displays detailed user information to the summary output.

Output

The following output is an example of user registration information, and Table 25: Output fields: security user describes the output fields.

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#
```

Table 25: Output fields: security user

Label	Description
User ID	Displays the name of a system user
Need new pwd	Y — The user must change their password at the next login N — The user is not forced to change their 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.

Label	Description
Password expires	Displays the number of days in which the user must change their login password
Attempted logins	Displays the number of times the user has attempted to login irrespective of whether the login succeeded or failed
Failed logins	Displays 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
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 login exec file which executes whenever the user successfully logs in to a console session

view

Syntax

view [*view-name*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays the SNMP MIB views.

Parameters

view-name

Specifies the name of the view to display output, up to 32 characters. If no view name is specified, the complete list of views is displayed.

detail

Displays detailed view information.

Output

The following output is an example of SNMP MIB view information, and Table 26: Output fields: security view describes the output fields.

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#
```

Table 26: Output fields: security view

Label	Description
view name	Displays the name of the view Views control the accessibility of a MIB object within the configured MIB view and subtree
oid tree	Displays the object identifier of the ASN.1 subtree
mask	Displays 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

2.9.2.2.2 Login control

users

Syntax

users

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays console user login and connection information.

Output

The following output is an example of console user login and connection information, and Table 27: Output fields: users describes the output fields.

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#
```

Table 27: Output fields: users

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

2.9.2.3 Debug commands

radius

Syntax

radius

no radius

Context

debug>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for RADIUS connections.

The **no** form of this command disables RADIUS debugging.

Default

no radius

detail-level

Syntax

detail-level {**low** | **medium** | **high**}

no detail-level

Context

debug>router>radius

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the RADIUS debugging output detail level.

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

Default

detail-level medium

Parameters

low

Specifies that the output include the packet type, server address, length, and RADIUS server policy name.

medium

Specifies that the output include the RADIUS attributes in the packets, in addition to all information included in low detail output.

high

Specifies that the output include hexadecimal packet dumps, in addition to all information included in medium and low detail output.

packet-type

Syntax

packet-type [**authentication**] [**accounting**] [**coa**]

no packet-type

Context

debug>router>radius

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the RADIUS packet types to include in the RADIUS debugging output.

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

Default

packet-type authentication accounting coa

Parameters

authentication

Specifies that RADIUS authentication packets should be included.

accounting

Specifies that RADIUS accounting packets should be included.

coa

Specifies that RADIUS change-of-authorization packets should be included.

radius-attr

Syntax

radius-attr type *attribute-type* [**transaction**]

radius-attr type *attribute-type* [**transaction**] {**address** | **hex** | **integer** | **string**} **value** *attribute-value*

radius-attr vendor *vendor-id* **type** *attribute-type* [**transaction**] [**encoding** *encoding-type*]

radius-attr vendor *vendor-id* **type** *attribute-type* [**transaction**] [**encoding** *encoding-type*] {**address** | **hex** | **integer** | **string**} **value** *attribute-value*

no radius-attr type *attribute-type*

no radius-attr type *attribute-type* {**address** | **hex** | **integer** | **string**} **value** *attribute-value*

no radius-attr vendor *vendor-id* **type** *attribute-type*

no radius-attr vendor *vendor-id* **type** *attribute-type* {**address** | **hex** | **integer** | **string**} **value** *attribute-value*

Context

debug>router>radius

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the RADIUS attributes to include in medium or high detail RADIUS debugging output.

The **no** form of this command disables the inclusion of the specified attributes.

Parameters

address

Specifies that the *attribute-value* is an IPv4 or IPv6 address, prefix, or subnet.

attribute-type

Specifies the RADIUS attribute type.

Values 1 to 255

attribute-value

Specifies the value of the RADIUS attribute.

Values **address** — *ipv4-address*, *ipv6-address*, *ipv6-prefix*/*prefix-length*

ipv4-address — a.b.c.d

ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)

ipv6-prefix — x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:d.d.d.d

x — 0 to FFFF (hexadecimal)

d — 0 to 255 (decimal)

prefix-length — 0 to 128
hex — 0x0 to 0xFFFFFFFF (up to 506 hexadecimal nibbles)

integer — 0 to 4294967295

string — ASCII string up to 253 characters

encoding-type

Specifies the size of the vendor-type and vendor-length in bytes. The information is configured in the format "xy", where "x" is the size of the vendor-type and "y" is the size of the vendor-length.

Values vendor-type — 1 to 4
vendor-length — 0 to 2

Default 11

hex

Specifies that the *attribute-value* is a binary string in hexadecimal format.

integer

Specifies that the *attribute-value* is an integer.

string

Specifies that the *attribute-value* is an ASCII string.

transaction

Specifies that the system outputs both request and response packets in the same session, even if the response packet does not include the filtered attributes.

vendor-id

Specifies the vendor ID for the vendor-specific attributes.

Values 0 to 16777215

server-address

Syntax

server-address *ip-address*

no server-address *ip-address*

Context

debug>router>radius

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the RADIUS server information to include in the RADIUS debugging output.

The **no** form of this command removes the specified RADIUS server from the RADIUS debugging output.

Parameters

ip-address

Specifies the IPv4 or IPv6 address of the RADIUS server.

Values *ipv4-address* — a.b.c.d

ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:d.d.d.d

x — 0 to FFFF (hexadecimal)

d — 0 to 255 (decimal)

3 SNMP

This chapter provides information to configure SNMP.

3.1 SNMP overview

This section provides an overview of SNMP information.

3.1.1 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.

3.1.2 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 management information consists of a set of network objects that can be managed with SNMP. Object identifiers are unique object names that are organized in a hierarchical tree structure. The main branches are defined by the Internet Engineering Task Force (IETF). When requested, the Internet Assigned Numbers Authority (IANA) assigns a unique branch for use by a private organization or company. The branch assigned to Alcatel-Lucent (TiMetra) is 1.3.6.1.4.1.6527.

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

3.1.3 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.

3.1.4 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.

3.1.5 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 be assigned community strings. 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-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.

The Nokia 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.

3.1.6 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.

3.1.7 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-managed objects controlled by the access rules associated with that view.

Predefined 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.

3.1.8 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.

3.1.9 Users

By default, authentication and encryption parameters are not configured. Authentication parameters which a user must use 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 whether 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).

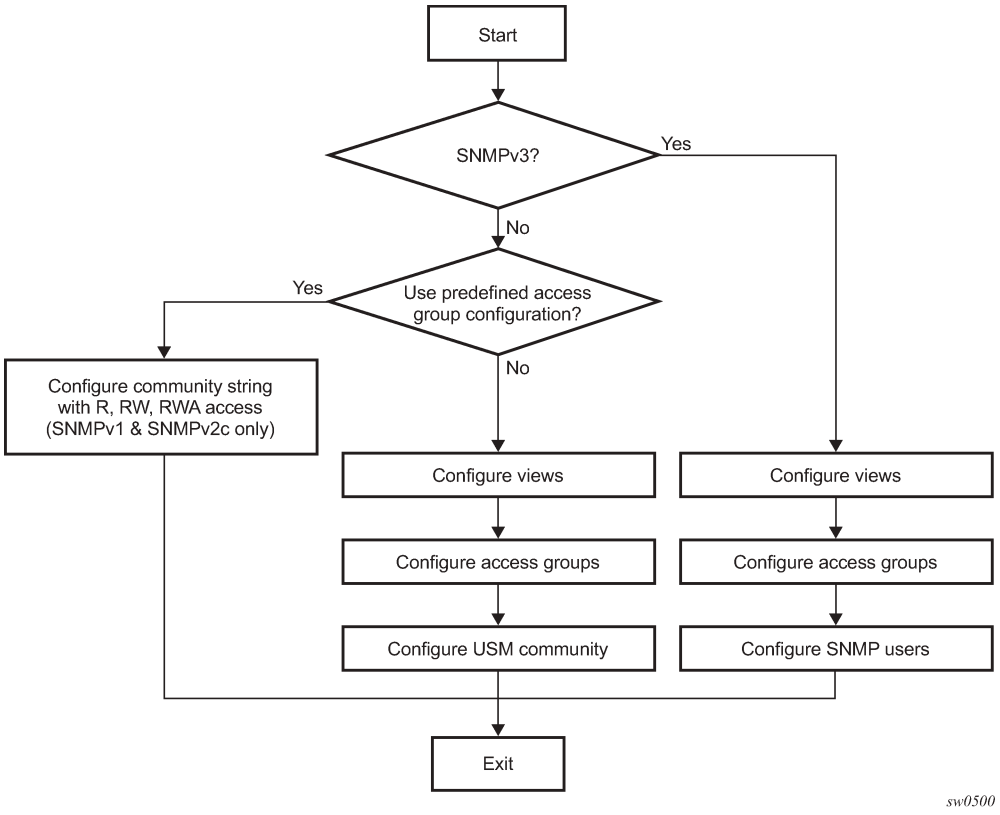
3.2 Which SNMP version to use

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 to be validated by the device. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine whether the message was tampered with.

The following figure shows the configuration requirements to implement SNMPv1/SNMPv2c, and SNMPv3.

Figure 5: SNMPv1 and SNMPv2c configuration and implementation flow



3.3 Configuration notes

This section describes SNMP configuration caveats.

3.3.1 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.

  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.

3.4 Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

3.4.1 SNMP configuration overview

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

3.4.1.1 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 predefined 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.

3.4.1.2 Configuring SNMPv3

The 7210 SAS implements SNMPv3 by default. If security features other than the default views are required, configure the following parameters:

- views
- access groups
- SNMP users
- SNMP engine ID

Note: When SNMPv3 is configured on the 7210 SAS-Sx/S 1/10GE (standalone-VC mode), use the **config>system>snmp>engineID** command to explicitly configure the SNMP engine ID. Failure to do so causes the SNMPv3 to stop working after a CPM switchover.

3.4.2 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

Example: 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-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
                attempts 20 time 5 lockout 10
```

3.4.3 Configuring SNMP components

Use the following syntax to configure SNMP scenarios.

```
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 security-level security-level
 [context context-name [prefix-match]] [read view-name-1] [write view-name-2] [notify view-
name-3]
```

3.4.3.1 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 preconfigured by the agent for SNMPv1/SNMPv2c.

Use the following syntax to configure community options.

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

Example: SNMP community configuration output

```
*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#
```

3.4.3.2 Configuring view options

Use the following syntax to configure view options.

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

Example: View configuration output

```
*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#
```

3.4.3.3 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 syntax to configure access features.

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

Example: Access configuration output

The following is a sample access configuration output 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 syntax to configure user group and authentication parameters.

```
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
```

Example: User SNMP configuration output

```
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#
```

3.4.3.4 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 syntax to configure USM community options.

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

Example: SNMP community configuration output

```
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.

3.4.3.5 Configuring other SNMP parameters

Use the following syntax to modify the system SNMP options.

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

Example: 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#
```

3.5 SNMP command reference

3.5.1 Command hierarchies

- Configuration commands
  - SNMP system commands
  - SNMP security commands
- Show commands

3.5.1.1 Configuration commands

3.5.1.1.1 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
```

3.5.1.1.2 SNMP security commands

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

The following commands configure user-specific SNMP features. See 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
```

3.5.1.2 Show commands

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

```
                - community [community-string]
            - ssh
            - users [user-id] [detail]
            - view [view-name] [detail]
```

3.5.2 Command descriptions

- Configuration commands
- Show commands

3.5.2.1 Configuration commands

- SNMP system commands
- SNMP security commands

3.5.2.1.1 SNMP system commands

engineID

Syntax

[**no**] **engineID** *engine-id*

Context

config>system>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

If the SNMP engine ID is changed using the **config**>**system**>**snmp**>**engineID** *engine-id* command, 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 that 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 SNMPv3 is configured on the 7210 SAS-Sx/S 1/10GE (standalone-VC mode), use the **config>system>snmp>engineID** command to explicitly configure the SNMP engine ID. Failure to do so causes the SNMPv3 to stop working after a CPM switchover.

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 this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the port number used by this node to receive SNMP request messages and to send replies.

Note:
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 this command reverts to the default value.

Default

general-port 161

Parameters

port-number

Specifies the port number used to send SNMP traffic other than traps.

Values 1 to 65535 (decimal)

packet-size

Syntax

packet-size *bytes*

no packet-size

Context

config>system>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 reverts to the default value.

Default

packet-size 1500

Parameters

bytes

Specifies the SNMP packet size in bytes.

Values 484 to 9216

snmp

Syntax

snmp

Context

config>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure SNMP parameters.

shutdown

Syntax

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

Context

config>system>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 in 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 this command administratively enables SNMP, which is the default state.

Default

no shutdown

3.5.2.1.2 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 command).

Default access group configurations cannot be modified or deleted.

To remove the user group with associated, security models, and security levels, use the **no access group** *group-name* command.

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

Parameters

group-name

Specifies 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 or privacy (encryption) is required. When configuring the user 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-1*

Specifies the name of the view, up to 32 characters, to read the MIB objects. This command must be configured for each view to which the group has read access.

write *view-name-2*

Specifies the name of the view, up to 32 characters, to configure the contents of the agent. This command must be configured for each view to which the group has write access.

notify *view-name-3*

Specifies the name of the view, up to 32 characters, to send a trap about MIB objects.This command must be configured for each view to which the group has notify access.

attempts

Syntax

attempts [*count*] [**time** *minutes1*] [**lockout** *minutes2*]

no attempts

Context

config>system>security>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 configured lockout time period.

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

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

Default

attempts 20 time 5 lockout 10

Parameters

count

Specifies the number of unsuccessful SNMP attempts allowed for the specified **time**.

Default 20

Values 1 to 64

time *minutes1*

Specifies 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 to 60

lockout *minutes2*

Specifies 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, that host is locked out from any further login attempts for the configured time period.

Default 10

Values 0 to 1440

community

Syntax

community *community-string* [**hash** | **hash2**] *access-permissions* [**version** *SNMP-version*]

no community *community-string*]

Context

config>system>security>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables 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, this command implies a security model for SNMPv1 and SNMPv2c only. For SNMPv3 security, the command must be configured.

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

Parameters

community-string

Specifies the SNMPv1 / SNMPv2c community string.

Values hash, hash2

access-permissions

Specifies the 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}

Specifies the scope of the community string 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

The mask value and 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 view subtree, both the included and the excluded, are defined in this table. To determine whether a particular object instance is in a particular MIB view, compare the OID with each of the MIB view active entries in this table. If none match, the object instance is not in the MIB view. If one or more match, 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.

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 1s)

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, the mask is extended with ones until the mask length matches the number of subidentifiers in the MIB subtree.

type {included | excluded}

Specifies whether to include or exclude MIB subtree objects.

Included means that all MIB subtree objects that are identified with a 1 in the mask are available in the view.

Excluded means that all MIB subtree objects that are identified with a 1 in the mask are denied access in the view.

Default included

snmp

Syntax

snmp

Context

config>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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.

The Nokia implementation of SNMP uses SNMPv3. To implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. To implement SNMP with security features (Version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views that specify more specific OIDs (MIB objects in the subtree) can be configured.

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

Parameters

community-string

Specifies the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used.

Values hash, hash2

group

Specifies the group that governs the access rights of this community string. This group must first be configured in the **config system security snmp access group** context.

view

Syntax

view *view-name* **subtree** *oid-value*

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

Context

config>system>security>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures a view. Views control the accessibility of an MIB object within the configured MIB view and subtree. OIDs uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.

When 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 for more information. The views 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.

Parameters

view-name

Specifies a view name up to 32 characters.

oid-value

Specifies the 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.

3.5.2.2 Show commands

counters

Syntax

counters

Context

show>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

The following output is an example of SNMP counter information, and Table 28: Output fields: SNMP counters describes the output fields.

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#
```

Table 28: Output fields: SNMP counters

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

Label	Description
variables set	Displays the number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs

information

Syntax

information

Context

show>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command lists the SNMP configuration and statistics.

Output

The following output is an example of SNMP configuration and statistics information, and Table 29: Output fields: system information describes the output fields.

Sample output

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

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

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

BOF Source             : cf1:
Image Source           : primary
Config Source          : primary
```

```
Last Booted Config File: ftp://172.22.184.249/./debby-sim1/debby-sim1-config.cfg
Last Boot Cfg Version  : THU FEB 15 16:58:20 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                         Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                         builder in /rel0.0/I1042/panos/main # Generated THU
                         FEB 11 16:58:20 2007 UTC
Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                         Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                         builder in /rel0.0/I1042/panos/main # Generated THU
                         FEB 15 16:58:20 2007 UTC
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: No
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script          : N/A
Cfg-OK Script Status   : not used
Cfg-Fail Script        : N/A
Cfg-Fail Script Status : not used

Management IP Addr     : 192.168.2.121/20
DNS Server             : 192.168.1.246
DNS Domain             : eng.timetra.com
BOF Static Routes      :
  To                   Next Hop
  172.16.10.0/23      192.168.1.251
  172.16.184.0/22      192.168.1.251
ATM Location ID        : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ATM OAM Retry Up       : 2
ATM OAM Retry Down     : 4
ATM OAM Loopback Period: 10
===============================================================================
A:ALA-1#
```

Table 29: Output fields: system information

Label	Description
System Name	Displays the name configured for the device
System Contact	Displays the text string that identifies the contact name for the device
System Location	Displays the text string that identifies the location of the device
System Coordinates	Displays 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	Displays the time since the last reboot
SNMP Port	Displays the port which SNMP sends responses to management requests

Label	Description
SNMP Engine ID	Displays the ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node
SNMP Max Message Size	Displays 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
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

Label	Description
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
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	Displays the maximum number of backup revisions maintained for a configuration file This value also applies to the number of revisions maintained for the BOF
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	Displays the Management IP address of the node
DNS Server	Displays the DNS address of the node
DNS Domain	Displays the DNS domain name of the node
BOF Static Routes	To — The static route destination

Label	Description
	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

access-group

Syntax

access-group *group-name*

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays access group information.

Output

The following output is an example of access group information, and Table 30: Output fields: access group describes the output fields.

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#
```

Table 30: Output fields: access group

Label	Description
Group name	Displays the access group name
Security model	Displays 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	Displays the total number of configured access groups

authentication

Syntax

authentication [**statistics**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays authentication information.

Output

The following output is an example of authentication information, and Table 31: Output fields: authentication describes the output fields.

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#
```

Table 31: Output fields: authentication

Label	Description
sequence	Displays the authentication order in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.
server address	Displays the address of the RADIUS, TACACS+, or local server
status	Displays the status of the server
type	Displays the server type
timeout (secs)	Displays the 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	Displays the number of attempts to retry contacting the server
radius admin status	Displays the administrative status of the RADIUS protocol operation
tacplus admin status	Displays 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	Displays the total number of servers configured

keychain

Syntax

keychain [*key-chain*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays keychain information.

Parameters

key-chain

Specifies the keychain name to display.

detail

Displays detailed keychain information.

Output

The following output is an example of keychain information, and Table 32: Output fields: keychain describes the output fields.

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#
```

Table 32: Output fields: keychain

Label	Description
TCP-Option number send	Displays the TCP option number to be inserted in the header of sent TCP packets
TCP-Option number receive	Displays the TCP option number that will be accepted in the header of received TCP packets

management-access-filter

Syntax

management-access-filter

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays management-access IP filters.

Parameters

entry-id

Displays information for the specified entry.

Values 1 to 9999

Output

The following output is an example of management access IP filter information, and Table 33: Output fields: IP filter describes the output fields.

Sample 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#
```

Table 33: Output fields: IP filter

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

Label	Description
Dest port	Displays the destination port
Match	Displays the number of times a management packet has matched this filter entry
Protocol	Displays the IP protocol to match
Action	Displays the action to take for packets that match this filter entry

password-options

Syntax

password-options

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays password options.

Output

The following output is an example of password option information, and Table 34: Output fields: password options describes the output fields.

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#
```

Table 34: Output fields: password options

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 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

profile

Syntax

profile [*profile-name*]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays user profiles for CLI command tree permissions.

Parameters

profile-name

Specifies the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names is displayed.

Output

The following output is an example of user profile information, and Table 35: Output fields: security profile describes the output fields.

Sample output

```
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#
```

Table 35: Output fields: security profile

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	Displays a text string describing the entry
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

snmp

Syntax

snmp

Context

show

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays SNMP information.

community

Syntax

community

community *community-string*

Context

show>system>security>snmp

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command lists SNMP communities and characteristics.

Parameters

community-string

Specifies the community name, up to 32 characters.

Output

The following output is an example of SNMP community information, and Table 36: Output fields: community describes the output fields.

Sample output

```
A:Dut-P# show system security snmp community
===============================================================================
Communities
===============================================================================
community           access  view                version   group name
-------------------------------------------------------------------------------
cli-readonly        r       iso                 v2c       cli-readonly
cli-readwrite       rw      iso                 v2c       cli-readwrite
private             rwa     iso                 v1 v2c    snmp-rwa
public              rwa     iso                 v1 v2c    snmp-rwa
```

```
-------------------------------------------------------------------------------
No. of Communities: 4
===============================================================================
A:Dut-P#
```

Table 36: Output fields: community

Label	Description
Community	Displays 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	Displays the view name
Version	Displays the SNMP version
Group Name	Displays the access group name
No of Communities	Displays the total number of configured community strings

ssh

Syntax

ssh

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays all the SSH sessions and the SSH status and fingerprint.

Output

The following output is an example of SSH session information, and Table 37: Output fields: SSH describes the output fields.

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#
```

Table 37: Output fields: SSH

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 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	Displays the IP address of the connected routers (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	Displays the name of the user
Number of SSH sessions	Displays the total number of SSH sessions

users

Syntax

users [*user-id*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays user information.

Output

The following output is an example of user information, and Table 38: Output fields: users describes the output fields.

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#
```

Table 38: Output fields: users

Label	Description
User ID	Displays the name of a system user
Need New PWD	Yes — The user must change their password at the next login No — The user is not forced to change their 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	Displays the date on which the current password expires
Attempted logins	Displays the number of times the user has attempted to login irrespective of whether the login succeeded or failed
Failed logins	Displays the number of unsuccessful login attempts
Local Conf.	Y — Password authentication is based on the local password database

Label	Description
	N — Password authentication is not based on the local password database

view

Syntax

view [*view-name*] [**detail**]

Context

show>system>security

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

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

Output

The following output is an example of MIB-OID tree views and permissions information, and Table 39: Output fields: security view describes the output fields.

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#
```

Table 39: Output fields: security view

Label	Description
View name	Displays the name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree
OID tree	Displays the Object Identifier (OID) value OIDs uniquely identify MIB objects in the subtree
Mask	Displays 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	Displays the total number of configured views
Group name	Displays the access group name

4 NETCONF

Note:
This feature is only supported on the 7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T.

This chapter describes the use of the Network Configuration Protocol (NETCONF) by the SR OS router to perform router management operations.

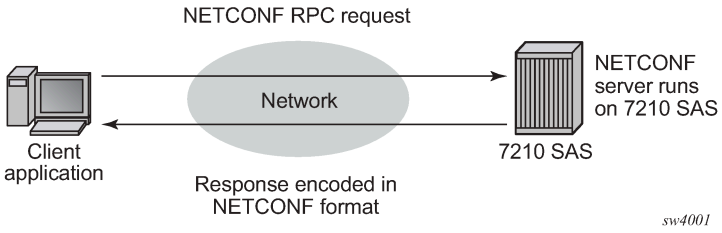
4.1 NETCONF overview

NETCONF is a standardized IETF configuration management and XML encoded protocol that can be used as an alternative to CLI or SNFMP to manage the SR OS routers. NETCONF is defined in RFC 6241, *NETCONF Configuration Protocol (NETCONF)*. It is secure and connection-oriented, and can run over the SSHv2 transport protocol, in accordance with RFC 6242, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*.

NETCONF uses Remote Procedure Call (RPC) messaging to facilitate communication between a NETCONF client and the NETCONF server that is running on the SR OS node. The RPC message and configuration data are encoded in an XML document. These XML documents are exchanged between the NETCONF client and a NETCONF server in a series of request and response type of messaging interactions. The SR OS NETCONF interface supports both configuration support and retrieval of operational information.

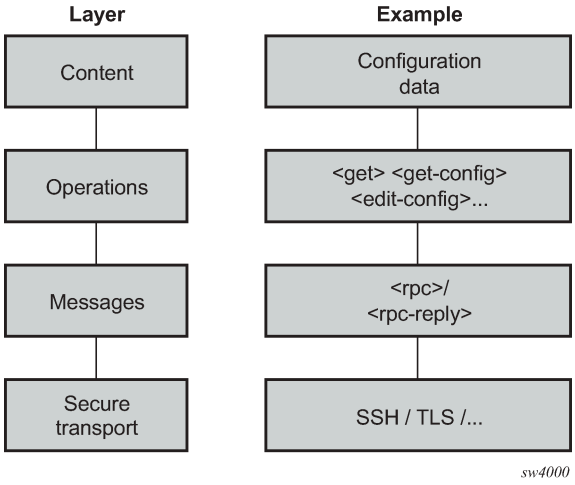
The following figure shows a NETCONF RPC messaging request.

Figure 6: NETCONF RPC request



As defined in RFC 6241, NETCONF can be conceptually partitioned into four layers; these are shown in the following figure.

Figure 7: NETCONF layers (RFC 6241)



4.2 NETCONF in SR OS

The SR OS router can use NETCONF to perform the following router management operations:

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

NETCONF is not used to generate notifications on an SR OS router; for example, log events, syslog, or SNMP notifications (traps).

The equivalent of some **admin** commands are available through the SR 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 through NETCONF on an SR OS router.

The SR OS NETCONF server supports both the base 1.1 and base 1.0 capabilities.

SR OS NETCONF supports both a CLI content layer and an XML-based content layer.

4.2.1 YANG data models

The SR OS NETCONF XML content layer configuration schema is described in a set of Alcatel-Lucent proprietary YANG modules. The configuration modules are advertised in the SR OS NETCONF server hello.

The configuration YANG data model closely aligns to the SR OS CLI configuration tree structure and commands.

A set of YANG modules are published and distributed as part of an SR OS image in the cflash/support directory (along with files like dictionary-freeradius.txt and stats.dtd).

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

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

4.2.2 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 (similar to CLI, Secure Copy (SCP), and SSH File Transfer Protocol (sFTP) sessions) are subject to any configurable and non-configurable session limits; for example, inbound-max-sessions. The SSH server and NETCONF protocol must be enabled in the router configuration to use NETCONF.

Unlike CLI sessions, NETCONF sessions are not subject to automatic session timeout. Operators can manually disconnect sessions using the **admin**>**disconnect netconf** command or the **admin**>**disconnect** command (terminates all SSH sessions).

NETCONF user accounts must exist on the SR OS to enable a client establishing a NETCONF session to log into the router. A new access type **netconf** is provided. The user must be configured with both **console** and **netconf** access.

Only authentication through the local user database is supported for NETCONF users (no RADIUS or TACACS+ authentication). Access to various CLI configuration and **show** commands (authorization) through NETCONF is controlled through the assigned user profile that is used to authenticate the underlying SSH session.

If a NETCONF request attempts to execute a CLI command that is outside the scope of its access profile, the system sends an error response.

Example

The following example shows a user request where the **show** command usage is outside the scope of the user's access profile.

```
<?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</cli-show>
                        </oper-data-format-cli-block>
                </filter>
        </get>
</rpc>
]]>]]>
```

The following example shows the 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'
            MINOR: CLI Command not allowed for this user.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

4.2.3 NETCONF operations

The following base protocol operations are supported:

- <get>
- <get-config>
- <edit-config>
- <copy-config>
- <delete-config>
- <validate>
- <close-session>
- <kill-session>

The <lock> and <unlock> base protocol operations are not supported.

The <error-option> operation is not supported. SR OS implements the stop-on-error behavior by default. The continue-on-error and rollback-on-error behaviors are not supported.

4.2.3.1 <get>

CLI content layer <get> operation is supported. XML content layer <get> operation is not supported.

A <get> request is analyzed for syntax errors before it is executed. If a syntax error is found, 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. A <response> tag containing the error information, followed by an <rpc-error> tag (and sub-tags) is attached to the erroneous item. The reply is returned, and no subsequent items are not executed.

For a non-syntax error, the <rpc-error> for an individual item is placed after the </response> information and not included in the <response> tag.

The following example shows a <get> request with a non-syntax error in the second 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.2.3.2 <get-config>

The <get-config> operation returns non-default configuration by default (that is, the "trim" mode, as defined in RFC 6243).

4.2.3.3 <edit-config>

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

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

4.2.3.4 <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> operation.

Remote URL-to-remote URL copies are not supported. For example, if the primary-image is a remote URL, 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> datastore.

4.2.3.5 <validate>

The following support is available for the validate:1.1 capability:

- The validate:1.1 and 1.0 capabilities are advertised in the NETCONF server <hello> as the following:
  - <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> operation is supported for a selection of config (<source><config>), or for the <running> datastore, which only returns 'OK'. The <validate> operation is not supported for URL sources or the <startup> datastore.

4.2.4 Datastores and URLs

The SR OS supports the following datastores:

- <running>
- <startup>
- <url>

Note:
<url> is not a datastore in itself.

The <candidate> datastore is not supported.

All configuration changes (<edit-config>) done to the <running> datastore through NETCONF take immediate operational effect.

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>, and others).

The :startup capability is advertised in the SR OS NETCONF server <hello> as follows:

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

The <url> tags support the same options as CLI <file-url>: local URLs (CF) and remote URLs (ftp and tftp).

The :url capability is advertised in the SR OS NETCONF server <hello> as follows:

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

The following examples show the format of each URL scheme:

Note:

- The examples use "///" for the file URL.
- The file://localhost/... format is not supported.

- <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>

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

The BOF is not considered to be part of any configuration datastore.

Debug configurations (such as **debug mirrors**, or configurations saved using the **admin debug-save** command) are not considered to be part of any configuration datastore.

Configuration changes made through NETCONF are subject to CLI rollback operations (**revert**, **save**, and so on) and are included in the configuration when an **admin save** operation is performed in the CLI.

4.2.5 General NETCONF behavior

Use **Ctrl-C** in a NETCONF session to immediately terminate the session.

The SR OS NETCONF implementation does not support XML namespaces (xmlns). Any XML namespace or prefix declarations in the RPC tag are accepted and returned in the <rpc-reply> tag, but are ignored and unused. Any XML namespace or prefix declarations in the rest of the request are ignored and unused. The SR OS NETCONF server puts the correct NETCONF namespace declaration ("urn:ietf:params:xml:ns:netconf:base:1.0") in all replies. See the following sections for more information:

- Example: multiple use of standard NETCONF namespace
- Example: non-standard namespace defined in <rpc> tag
- Example: non-standard namespace not defined in <rpc> tag
- Example: non-standard namespace or prefix not defined in <rpc> tag

The chunked framing mechanism is supported in addition to the EOM mechanism. As described in 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 old end-of-message-based mechanism (see Section 4.3) is used." See Example: chunked frame mechanism for more information.

Default data handling (for example, **info** vs **info detail**) is supported in accordance with the mechanisms detailed in RFC 6243. The SR OS NETCONF server supports the "trim" method and advertises it in the <hello> as follows:

```
<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=trim</
capability>
```

Pseudo-transactional capabilities are supported. A user can save a rollback checkpoint (for example, before performing an <edit-config> or a series of <edit-config>) and, if required, later perform a rollback revert. See the following sections for more information:

- Example: two rollback items with responses
- Example: syntax error in the rollback request
- Example: error in processing the request
- Example: error in second item of the request

4.2.5.1 Example: multiple use of standard NETCONF namespace

Example

The following example shows the standard NETCONF namespace "urn:ietf:params:xml:ns:netconf:base:1.0" 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>
        <router>
            <interface>
               <interface-name>"system"</interface-name>
            </interface>
        </router>
    </configure>
</filter>
</get-config>
</rpc>
]]>]]>
```

In the following reply, the namespace is accepted and no error message is returned.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-
id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:
xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-name>Base</router-name>
                <interface>
                    <interface-name>system</interface-name>
                    <address>
                        <ip-address-mask>144.23.63.5/32</ip-address-mask>
                    </address>
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

4.2.5.2 Example: non-standard namespace defined in <rpc> tag

Example

The following example shows a non-standard NETCONF base namespace defined in the <rpc> tag.

```
<?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>
]]>]]>
```

In the following reply, the non-standard namespace used in the <rpc> 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:alcatel-
lucent.com:sros:ns:yang:conf-r13">
<data>
     <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
          <router>
               <router-name>Base</router-name>
               <interface>
                    <interface-name>system</interface-name>
                    <address>
                         <ip-address-mask>144.23.63.5/32</ip-address-mask>
                    </address>
                    <shutdown>false</shutdown>
               </interface>
          </router>
     </configure>
</data>
</rpc-reply>
]]>]]>
```

4.2.5.3 Example: non-standard namespace not defined in <rpc> tag

Example

The following example shows a non-standard NETCONF namespace used in one of the tags, but not defined in the <rpc> tag.

```
<?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>
        <router>
            <interface xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
                 <interface-name>"system"</interface-name>
            </interface>
        </router>
    </configure>
</filter>
</get-config>
</rpc>
]]>]]>
```

In the following reply, the non-standard namespace used in the tag is ignored.

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

```
id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:
xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-name>Base</router-name>
                <interface>
                    <interface-name>system</interface-name>
                    <address>
                        <ip-address-mask>144.23.63.5/32</ip-address-mask>
                    </address>
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

4.2.5.4 Example: non-standard namespace or prefix not defined in <rpc> tag

Example

The following example shows a non-standard NETCONF namespace or prefix used in one of the tags but not defined in the <rpc> tag.

```
<?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>
        <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>
]]>]]>
```

In the following reply, the non-standard namespace/prefix used in tag is ignored.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-
id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:
xml:ns:netconf:base:1.0">
    <data>
        <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <router>
                <router-name>Base</router-name>
                <interface>
                    <interface-name>system</interface-name>
                    <address>
                        <ip-address-mask>144.23.63.5/32</ip-address-mask>
                    </address>
```

```
                    <shutdown>false</shutdown>
                </interface>
            </router>
        </configure>
    </data>
</rpc-reply>
]]>]]>
```

4.2.5.5 Example: chunked frame mechanism

Example

The following example shows a chunked message.

```
#302
<?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><configure><router><interface><interface-name>system</
interface-name></interface></router></configure></config></filter></get-config></
rpc>
##
```

The following example shows the reply.

```
#38
<?xml version="1.0" encoding="UTF-8"?>
#85
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
#62
    <source><running/></source>
    <filter>
      <configure>
##79
        <system>
            <netconf>
            </netconf>
        </system>
##55
      </configure>
    </filter>
  </get-config>
</rpc>
##
```

4.2.5.6 Example: two rollback items with responses

Example

The following example shows 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.2.5.7 Example: syntax error in the rollback request

Example

The following example shows a syntax error in the request, which results in a 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.2.5.8 Example: error in processing the request

Example

The following example shows an 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.2.5.9 Example: error in second item of the request

Example

The following example shows an error in the second item of the request, resulting in no third 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.2.5.10 System provisioned configuration objects

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

Some of these SPC objects can be deleted or removed by a user (deletable system provisioned configuration (SPC) objects):

- In CLI, the SPC objects are removed by specifying the keyword **no**, which is then visible in an **info** command or in a saved configuration (**admin save**); for example, `no log-id 99`.
- The deletable SPC objects can be removed or recreated using NETCONF <edit-config> requests, but they are not visible in a <get-config> response if 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 if a child leaf or object is changed from the default value; for example, changing log-99 to time-format local.
- 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 they cannot be deleted, some of these non-deletable objects contain modifiable leaves.

- The non-deletable SPC objects are not visible in a <get-config> response when the SPC objects are set to their default values, including all child leaves and objects.
- The non-deletable SPC objects are visible in a <get-config> response if a child leaf or object is changed from the default value; for example, setting the **card-type**.
- 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, even if they are set to default values:

Example

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

4.3 Establishing a NETCONF session

Example

The following example shows a client on a Linux PC initiating a connection to an SR OS NETCONF server. In accordance with RFC 6242, the SSH session must be invoked using an SSH subsystem.

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

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

Example

The following is a message from the SR 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: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</capability>
        <capability>urn:ietf:params:xml:ns:netconf:base:1.0?module=ietf-
netconf&amp;revision=2015-02-27&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=2015-02-27</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-
r13?module=alu-cli-content-layer-r13&amp;revision=2015-02-27</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-r13?module=conf-
r13&amp;revision=2015-02-27</capability>
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-aaa-r13?module=conf-
aaa-r13&amp;revision=2015-02-27</capability>
...
...
...
...
        <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-vsm-r13?module=conf-
vsm-r13&amp;revision=2015-02-27</capability>
    </capabilities>
    <session-id>54</session-id>
</hello>
]]>]]>
```

The following is a reply from a NETCONF client.

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

4.4 XML content layer

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

The XML formatted configuration information must be correctly ordered and has the same dependencies and behavior as the equivalent CLI commands.

4.4.1 <edit-config> with XML content layer

An <edit-config> operation is supported with the <running> datastore only. The following <edit-config> operation attribute values are supported:

- merge
- remove
- delete
  - 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
- create
  - 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.

The "replace" operation is not supported as an attribute value for the <edit-config> operation.

Both "delete" and "remove" operations have the following behavior:

- Delete or remove operations are not supported for boolean leaves. For example, any of the following samples 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> can be used instead to make the request valid:

- A <delete> or <remove> operation is the equivalent of the **no** command in CLI. This **no** command is applied whether the default for the command is enabled, disabled (**no**), or a specific value. The delete operation is not aware of the default value of the object/leaf being deleted.
- A <delete> or <remove> operation for a leaf, where the request also specifies a value for the leaf, will result in an error.

The <edit-config> <default-operation> parameter is supported merge and none values. The "replace" value is not supported. 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.

For merge and create operations, the operations and tags specified in an <edit-config> request are order-aware and order-dependent, and the sequence of operations must follow the required sequence of the equivalent CLI commands. The <edit-config> is processed and executed in a top-down order. The same leaf can be enabled, disabled, or enabled and then disabled, and the final result is whatever was last specified for that leaf in the <edit-config> request.

For <delete> and <remove> operations, the SR 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. If children branches of an object must be removed before deleting the object in CLI, the equivalent delete request in a NETCONF <edit-config> must contain all those children if they exist, such as if the children are configured in the config datastore).

Example

In the following example, SR OS shuts down the test interface, deletes the interface, shuts down the VPLS, and removes it.

```
<config>
    <configure>
        <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>
```

Note:
The 'operation="merge"' is required in the shutdown nodes; otherwise, the inherited operation is <delete>, which is not supported on boolean leaves.

In the preceding example, if other children of "vpls 11" exist in the config besides the interface test specified in the delete request, and it is required to delete those children in CLI before "vpls 11" is removed, the deletion request fails. All configured children must be specified in the delete request.

4.4.2 <get-config> with XML content layer

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

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

The subtree filtering behavior is as follows:

- Attribute match expressions, as defined in section 6.2.2 of RFC 6241, are not supported.
- Only containers are supported as selection nodes, as defined in 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, without also specifying the key, 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, as defined in 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).

A <get-config> request 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.

See the following sections for examples of <get-config> request and response messages:

- Example: request that returns an error
- Example: content match node on a list key
- Example: selection node that is a container
- Example: list name node as an invalid selection node
- Example: empty leaf node as invalid selection node
- Example: key repeated in the same instance of the list node
- Example: retrieving the full configuration

4.4.2.1 Example: request that returns an error

Example

The following example shows a request that returns an error.

```
<?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>
                               <router>
                                       <interface>
                                               <interface-name>abc</interface-name>
                                               <delayed-enable>30</delayed-enable>
                                       </interface>
                               </router>
                       </configure>
               </filter>
       </get-config>
</rpc>
]]>]]>
```

The following example shows the 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 "abc" delayed-enable'
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

4.4.2.2 Example: content match node on a list key

Multiple key leaves 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

The following example shows a valid <get-config> request for a content match node 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>
        <router>
            <interface>
                <interface-name>abc</interface-name>
            </interface>
        </router>
    </configure>
   </filter>
        </get-config>
</rpc>
]]>]]>
```

4.4.2.3 Example: selection node that is a container

Example

The following example shows 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>
                 <router/>
             </configure>
         </filter>
    </get-config>
</rpc>
]]>]]>
```

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

4.4.2.4 Example: list name node as an invalid selection node

Example

The following example shows an invalid <get-config> request for a list name node that is an 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>
                                       <router>
                                               <interface>
                                               </interface>
                                       </router>
                               </configure>
                       </filter>
       </get-config>
</rpc>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.4.2.5 Example: empty leaf node as invalid selection node

Example

The following example shows an invalid <get-config> request for an empty leaf node that is an 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>
                <system>
                        <security>
                                    <ftp-server>
                                                </ftp-server>
                                    </security>
                         </system>
                 </configure>
            </filter>
        </get-config>
</rpc>
]]>]]>
```

The following example shows the 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>bad-element</error-tag>
        <error-severity>error</error-severity>
        <error-info>
            <bad-element>ftp-server</bad-element>
        </error-info>
        <error-message>
            Element is not valid in the specified context.
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

4.4.2.6 Example: key repeated in the same instance of the list node

Example

The following example shows an invalid <get-config> request for a key that is 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>
                                <router>
                                        <interface>
                                                <interface-name>abc</interface-name>
                                                <interface-name>def</interface-name>
                                        </interface>
                                </router>
                        </configure>
                </filter>
        </get-config>
</rpc>
]]>]]>
```

The following example shows the 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 "abc" "def"'
        </error-message>
    </rpc-error>
</rpc-reply>
]]>]]>
```

4.4.2.7 Example: retrieving the full configuration

The full configuration (equivalent to the CLI command **admin display-config**) can be retrieved using a <get-config> request:

- when the <filter> tag is not present

Example

```
<get-config>
    <source>
         <running/>
    </source>
</get-config>
```

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

Example

```
<get-config>
     <source>
          <running/>
     </source>
     <filter>
          <configure/>
     </filter>
</get-config>
```

4.5 XML content layer examples

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

4.5.1 Example: checking NETCONF status

The following example shows a <get-config> request and response to check whether NETCONF is shut down on the router.

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

The following example shows the 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>
]]>]]>
```

4.5.2 Example: creating a basic VPRN service

Example

The following example shows a <edit-config> request and response 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>
                <service>
                    <vprn operation="create">
                        <service-id>200</service-id>
                        <customer>1</customer>
                    </vprn>
```

```
                </service>
            </configure>
        </config>
  </edit-config>
</rpc>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.5.3 Example: creating a VPRN service with a SAP

Example

The following example shows a <edit-config> request and response to create a basic VPRN service with a SAP; the system creates the service/interface, but fails to create the SAP because the specified port 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>
                <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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.6 CLI content layer

When the CLI format is used at the NETCONF content layer, configuration changes and 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> request is significant and affects the processing of the CLI commands, such as which CLI branch is considered the "working context". In the following two examples the "working context" after the commands 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 made using NETCONF trigger the same "change" log events (for example, tmnxConfigCreate) as a normal CLI user doing the same changes.

The <with-defaults> tag, as defined in 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 using 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>. The <report-all> tag is not supported.

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

See CLI content layer examples for more information.

4.7 CLI content layer examples

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

4.7.1 Example: configuration change

Example

The following example shows 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 SR 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.7.2 Example: retrieving configuration information

Example

The following example shows 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.7.3 Example: retrieving full configuration information

Example

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 fill 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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.7.4 Example: <get> request

Example

The following example shows a <get> request.

```
<?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>
]]>]]>
```

The following example shows the 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>
]]>]]>
```

4.8 NETCONF command reference

4.8.1 Command hierarchies

4.8.1.1 Configuration commands

4.8.1.1.1 Netconf system commands

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

4.8.1.1.2 Netconf security commands

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

4.8.1.1.3 Show commands

```
show
    - system
        - netconf
            - counters
```

4.8.2 Command descriptions

4.8.2.1 Configuration commands

This section provides NETCONF configuration command descriptions.

4.8.2.2 NETCONF system commands

shutdown

Syntax

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

Context

config>system>netconf

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

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.

4.8.2.3 NETCONF security commands

netconf

Syntax

netconf

Context

config>system>security>profile

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

Description

Commands in this context authorize various NETCONF capabilities for the user.

base-op-authorization

Syntax

base-op-authorization

Context

config>system>security>profile>netconf

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

Description

Commands in this context configure where permission to use various NETCONF operations is controlled.

kill-session

Syntax

[**no**] **kill-session**

Context

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

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

Description

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

The **no** form of this command disables the configuration.

Default

no kill-session

4.8.2.4 Show commands

netconf

Syntax

netconf

Context

show>system

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

Description

This command displays active NETCONF SSH sessions.

Output

The following output is an example of NETCONF SSH session information, and Table 40: Output fields: NETCONF describes the output fields.

Sample output

```
7210SAS>show>system# netconf

===============================================================================
NETCONF Server
===============================================================================
Administrative State      : Disabled
Operational State         : Down
===============================================================================
```

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

Table 40: Output fields: NETCONF

Label	Description
Administrative State	Enabled — Indicates that NETCONF is enabled Disabled — Indicates that NETCONF is disabled
Operational State	Up — Indicates that NETCONF is operational Down — Indicates that NETCONF is not operational
Connection	Displays the IP address of the connected routers (remote client)

counters

Syntax

counters

Context

show>system>netconf

Platforms

7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-T

Description

This command displays NETCONF counters.

Output

The following output is an example of NETCONF counter information, and Table 41: Output fields: NETCONF counters describes the output fields.

Sample output

```
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#
```

Table 41: Output fields: NETCONF counters

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

5 Event and accounting logs

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

5.1 Logging overview

The two primary types of logging supported in the 7210 SAS OS are event logging and accounting logs.

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The 7210 SAS groups events into three major categories or event sources:

- **Security events**

  Events that pertain to attempts to breach system security.
- **Change events**

  Events that pertain to the configuration and operation of the node.
- **Main events**

  Events that pertain to applications that are not assigned to other event categories/sources.
- **Debug events**

  Events that pertain to trace or other debugging information.

The following are events within the 7210 SAS and have the following characteristics:

- a time stamp in UTC or local time
- the generating application
- a unique event ID within the application
- the VRF-ID
- a subject identifying the affected object
- a short text description

Event control assigns the severity for each application event and whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7210 SAS OS conform to ITU standards M.3100 X.733 and X.21 and are listed in the following table.

Table 42: Event severity levels

Severity number	Severity name
1	cleared
2	indeterminate (info)
3	critical

Severity number	Severity name
4	major
5	minor
6	warning

Events that are suppressed by event control will not generate any event log entries. Event control maintains a count of the number of events generated (logged) and dropped (suppressed) for each application event. The severity of an application event can be configured in event control.

An event log within the 7210 SAS OS associates the event sources with logging destinations. Examples of logging destinations include, the console session, a specific Telnet or SSH session, memory logs, file destinations, SNMP trap groups and syslog destinations. A log filter policy can be associated with the event log to control which events will be logged in the event log based on combinations of application, severity, event ID range, VRF ID, and the subject of the event.

The 7210 SAS accounting logs collect comprehensive accounting statistics to support a variety of billing models. The routers collect accounting data on services and network ports on a per-service class basis. In addition to gathering information critical for service billing, accounting records can be analyzed to provide insight about customer service trends for potential service revenue opportunities. Accounting statistics on network ports can be used to track link utilization and network traffic pattern trends. This information is valuable for traffic engineering and capacity planning within the network core.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to access objects (such as access ports and SAPs or network objects (such as SDPs, network ports, network IP interface). Accounting statistics are collected by counters for individual service meters defined on the customer 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 allows the user to 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 the 7210 SAS-T.

5.2 Log destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination.

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.

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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. Therefore, complying to this rule is subject to the incoming rate of the data being logged. For example, if the rate is very low, the actual rollover time may be longer than the configured value.

The retention time for a log file specifies the amount of time the file should be retained on the system based on the creation date and time of the file. The system continuously checks for log files with expired retention periods once every hour and deletes as many files as possible during a ten second interval.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file.

Event log files are always created in the `\log` directory on the specified compact flash device. The naming convention for event log files is:

log *eeff-timestamp*

where:

- *ee* is the event log ID
- *ff* is the log file destination ID
- *timestamp* is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:
  - *yyyy* is the four-digit year (for example, 2017)
  - *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`.

5.2.5 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.

5.2.6 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. The following table lists the severity level mappings to syslog severities.

Table 43: 7210 SAS to syslog severity level mappings

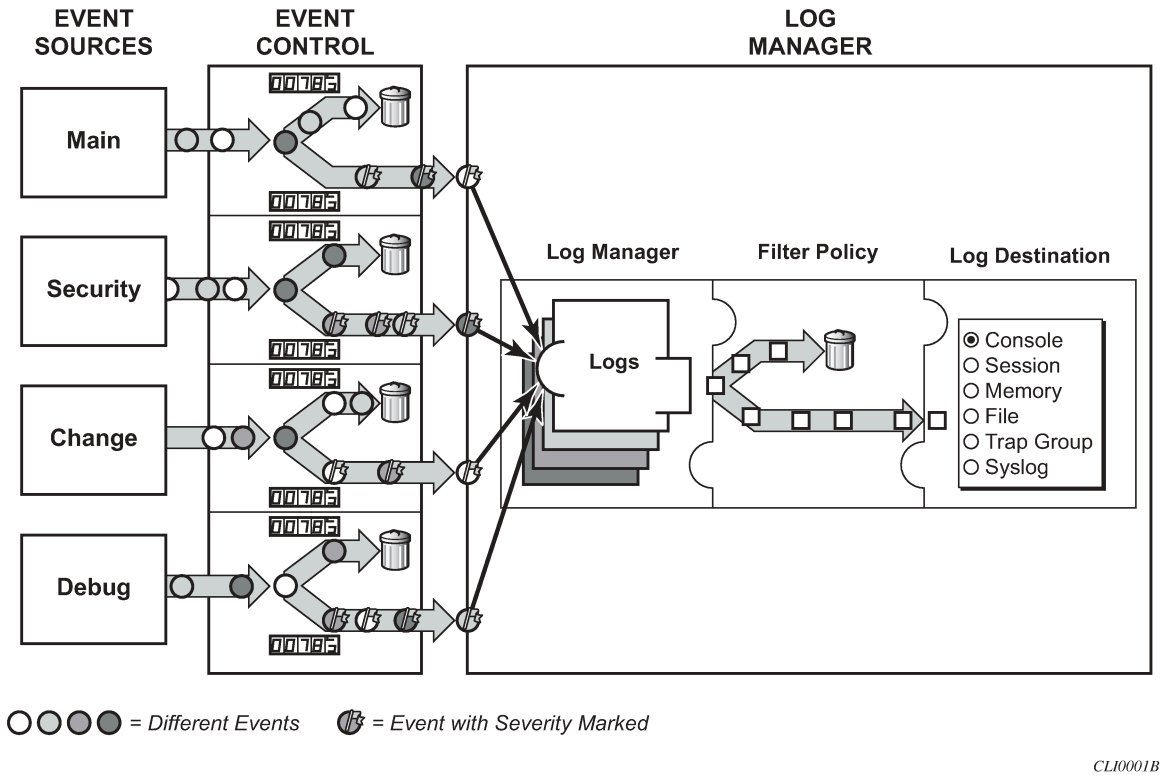
Severity level	Numerical severity (highest to lowest)	Syslog configured severity	Definition
—	0	emergency	System is unusable
critical (3)	1	alert	Action must be taken immediately
major (4)	2	critical	Critical conditions
minor (5)	3	error	Error conditions
warning (6)	4	warning	Warning conditions
—	5	notice	Normal but significant condition
cleared (1) indeterminate (2)	6	info	Informational messages
—	7	debug	Debug-level messages

5.3 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.

The following figure shows a function block diagram of event logging.

Figure 8: Event logging block diagram



5.3.1 Event sources

In Figure 8: Event logging block diagram, 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, and so on.

Example

The following output is 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#
```

5.3.2 Event control

Event control preprocesses 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.

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 describes why the event is generated. The event number is unique within an application, but the number can be duplicated in other applications.

Example

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#
```

5.3.3 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.

5.3.4 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 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 described in the following table.

Table 44: Valid 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 specific 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

5.3.5 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
```

Example: Event log

```
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 the following table.

Table 45: 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.

Label	Description
	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)
<application>	The application generating the log message.
<event_id>	The application 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.

5.3.6 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. When 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.

5.3.7 Default system log

Log 99 is a preconfigured memory-based log which logs events from the main event source (not security, debug, and so on). Log 99 exists by default.

Example: Log 99 configuration output

```
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#
```

5.4 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 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.

5.4.1 Accounting records

An accounting policy must define a record name and collection interval. Only one record name can be configured per accounting policy. Also, a record name can only be used in one accounting policy.

The record name, sub-record types, and default collection period for access and network accounting policies are shown as follows.

The 7210 SAS provides 21 accounting records for the following accounting policies:

- access
- accessport
- network
- networkIf
- sdp

When creating accounting policies, only one (of each) access, accessport, network, networkIf and sdp accounting policy can be defined as default. If statistics collection is enabled on an accounting object and no accounting policy is applied, the default accounting policy is used. If a default policy is not defined, no statistics are collected unless a specifically defined accounting policy is applied.

Each accounting record name is composed of one or more sub-records composed of multiple fields.

For VLL and VPLS services on the 7210 SAS, the user can run the **config>service>epipe/vpls>sap>statistics>ingress>counter-mode** {**in-out-profile-count** | **forward-drop-count**} to change the **counter-mode** of counters associated with SAP ingress meters or policers. See the *7210 SAS-Mxp, S, Sx, T Services Guide* and *7210 SAS-R6, R12 Services Guide* for more information about the **counter-mode** command.

The statistics collected for the following accounting records vary based on the counter-mode selected:

- Service-ingress-octets
- Service-ingress-packets
- Combined-service-ingress
- Complete-service-ingress-egress

See Appendix: accounting record name details for 7210 SAS platforms for more information about accounting records and counters for the 7210 SAS platforms.

5.4.2 Configuration guidelines

Before modifying the counter, disable account log generation. Execute the **no collect-stats** command. Changing the mode of the counter results in loss of previously collected counts and resets the counter.

5.4.3 Accounting files

When a policy has been created and applied to a service or network port, the accounting file is stored on the compact flash in a compressed XML file format. The device creates two directories on the compact flash to store the files.

Example

The following output displays a directory named act-collect that holds accounting files that are open and actively collecting statistics. The directory named act stores the files that have been closed and are awaiting retrieval.

```
ALA-1>file cf1:\# dir act*
12/19/2006 06:08a <DIR> act-collect
12/19/2006 06:08a <DIR> act

ALA-1>file cf1:\act-collect\ # dir
Directory of cf1:\act-collect#
12/23/2006 01:46a <DIR> .
12/23/2006 12:47a <DIR>  ..
12/23/2006 01:46a 112 act1111-20031223-014658.xml.gz
12/23/2006 01:38a 197 act1212-20031223-013800.xml.gz
```

Accounting files always have the prefix act followed by the accounting policy ID, log ID and timestamp. The accounting log file naming and log file destination properties like rollover and retention are described in more detail in Log files.

5.4.4 Design considerations

When preparing for an accounting policy deployment, verify that data collection, file rollover, and file retention intervals are properly tuned for the amount of statistics to be collected.

If the accounting policy collection interval is too brief, there may be insufficient time to store the data from all the services within the specified interval. If that is the case, some records may be lost or incomplete. Interval time, record types, and number of services using an accounting policy are all factors that should be considered when implementing accounting policies.

The rollover and retention intervals on the log files and the frequency of file retrieval must also be considered when designing accounting policy deployments. The amount of data stored depends on the type of record collected, the number of services that are collecting statistics, and the collection interval that is used.

5.5 Configuration notes

This following information describes logging configuration restrictions:

- 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**.

5.6 Configuring logging with CLI

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

5.6.1 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

5.6.1.1 Log types

Logs can be configured in the following contexts:

- **Log file**

Log files can contain log event message streams or accounting/billing information. Log file IDs are used to direct events, alarms/traps and debug information to their respective targets.

- **SNMP trap groups**

  SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.

- **Syslog**

  Information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element.

- **Event control**

  Configures a particular event or all events associated with an application to be generated or suppressed.

- **Event filters**

  An event filter defines whether to forward or drop an event or trap based on match criteria.

- **Accounting policies**

  An accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more s access object or network objects.

- **Event logs**

  An event log defines the types of events to be delivered to its associated destination.

- **Event throttling rate**

  Defines the rate of throttling events.

5.6.2 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

Example: Configuration output

```
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#
```

5.6.3 Common configuration tasks

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

5.6.3.1 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 syntax to configure a log file.

```
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
```

Example: Log file configuration output

```
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#
```

5.6.3.2 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 syntax to configure a log file.

```
config>log
        file-id log-file-id
            description description-string
            location cflash-id
            rollover minutes [retention hours]
```

For the 7210 SAS-T:

```
config>log
        file-id log-file-id
            description description-string
            location cflash|usb-flash-id [backup-cflash-id]
            rollover minutes [retention hours]
```

Example: Log file configuration output

```
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#
```

5.6.3.3 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 and Configuring a file ID.

Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one access, one access port, one network, one network interface and one SDP accounting policy can be defined as default. If statistics collection is enabled on an accounting object, and no accounting policy is applied, then the respective default accounting policy is used. If no default policy is defined, then no statistics are collected unless a specifically-defined accounting policy is applied.

Use the following syntax to configure an accounting policy.

```
config>log>
        accounting-policy acct-policy-id interval minutes
            description description-string
            default
            record record-name
            to file log-file-id
```

```
            no shutdown
```

Example: Accounting policy configuration output

```
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#
```

5.6.3.4 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.

```
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]
```

Example: Event control configuration output

```
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#
```

5.6.3.5 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 syntax to configure the throttle rate.

```
config>log#
        throttle-rate events [interval seconds]
```

Example: Throttle rate configuration output

```
*A:gal171>config>log# info
```

```
-----------------------------------------
        throttle-rate 500 interval 10
        event-control "aps" 2001 generate throttle
-----------------------------------------
```

5.6.3.6 Configuring a log filter

Use the following syntax to configure a log filter.

```
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]
```

Example: Log filter configuration output

```
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#
```

5.6.3.7 Configuring an SNMP trap group

The associated *log-id* does not have to be configured before an **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 syntax to configure an SNMP trap group.

```
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}]
```

Example: SNMP trap group configuration output

```
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#
```

5.6.3.8 Configuring SNMP dying gasp

Note:

- SNMP dying gasp for IPv4 is supported on all 7210 SAS platforms as described in this document, except the 7210 SAS-R6 and 7210 SAS-R12.
- SNMP dying gasp for IPv6 is not supported on any of the 7210 SAS platforms.

Use the following syntax to configure SNMP dying gasp.

```
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}]]
```

Example

```
*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 10.1.1.1 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 10.2.2.2 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#
```

5.6.3.8.1 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. Nokia recommends that users run a periodic ping query to the SNMP trap server in the background using the cron utility.

Example

The following is a sample configuration output 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#
```

5.6.3.9 Configuring a syslog target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

Use the following syntax to configure a syslog file.

```
config>log
        syslog syslog-id
            description description-string
            address ip-address
            log-prefix log-prefix-string
            port port
            level {emergency|alert|critical|error|warning|notice|info|debug}
            facility syslog-facility
```

Example: Syslog configuration output

```
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#
```

5.6.4 Log management tasks

This section describes the logging tasks.

5.6.4.1 Modifying a log file

Use the following syntax to modify a log file.

```
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
```

Example: Current log configuration output

```
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#
```

Example: Command usage to modify log file parameters

```
  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
```

Example: Modified log file configuration output

```
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#
```

5.6.4.2 Deleting a log file

The log ID must be shut down first before it can be deleted. In the previous example, "file 1" is associated with "log-id 2".

Example

```
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 syntax to delete a log file.

```
config>log
        no log-id log-id
        shutdown
```

Example: Command usage to delete a log file

```
  config# log
 config>log# log-id 2
 config>log>log-id# shutdown
 config>log>log-id# exit
 config>log# no log-id 2
```

5.6.4.3 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 syntax to modify a log file.

```
config>log
        file-id log-file-id
            description description-string
            location [cflash-id]
            rollover minutes [retention hours]
```

Example: Current log configuration output

```
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#
```

Example: Command usage to modify log file parameters

```
  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
```

Example: File modifications

```
A:ALA-12>config>log# info
----------------------------------------------
...
file-id 1
            description "LocationTest."
            location cf1:
            rollover 2880 retention 500
        exit
...
----------------------------------------------
```

5.6.4.4 Deleting a file ID

Note:
All references to the file ID must be deleted before the file ID can be removed.

Use the following syntax to delete a log ID.

```
config>log
        no file-id log-file-id
```

Example: Command usage to delete a file ID

```
config>log# no file-id 1
```

5.6.4.5 Modifying a syslog ID

Note:
All references to the syslog ID must be deleted before the syslog ID can be removed.

Use the following syntax to modify a syslog ID parameters.

```
config>log
        syslog syslog-id
            description description-string
            address ip-address
            log-prefix log-prefix-string
            port port
            level {emergency|alert|critical|error|warning|notice|info|debug}
            facility syslog-facility
```

Example: Command usage to modify syslog ID parameters

```
 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
```

Example: Syslog configuration output

```
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#
```

5.6.4.6 Deleting a syslog

Use the following syntax to delete a syslog file.

```
config>log
        no syslog syslog-id
```

Example: Command usage to delete a syslog ID

```
  config# log
 config>log# no syslog 1
```

5.6.4.7 Modifying an SNMP trap group

Use the following syntax to modify an SNMP trap group.

```
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}]
```

Example: Current SNMP trap group configuration output

```
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#
```

Example: Command usage to modify an SNMP trap group

```
  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"
```

Example: SNMP trap group configuration output

```
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#
```

5.6.4.8 Deleting an SNMP trap group

Use the following syntax to delete a trap target and SNMP trap group.

```
config>log
        no snmp-trap-group log-id
            no trap-target name
```

Example: SNMP trap group configuration output

```
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#
```

Example: Command usage to delete a trap target and SNMP trap group

```
 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
```

5.6.4.9 Modifying a log filter

Use the following syntax to modify a log filter.

```
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]
```

Example: Current log filter configuration output

```
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#
```

Example: Command usage to modify the log filter

```
 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
```

Example: Sample log filter configuration output

```
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#
```

5.6.4.10 Deleting a log filter

Use the following syntax to delete a log filter.

```
config>log
        no filter filter-id
```

Example: Current log filter configuration output

```
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#
```

Example: Command usage to delete a log filter

```
   config>log# no filter 1
```

5.6.4.11 Modifying event control parameters

Use the following syntax to modify event control parameters.

```
config>log
        event-control application-id [event-name|event-number] generate [severity-level]
 [throttle]
        event-control application-id [event-name|event-number] suppress
```

Example: Current event control configuration output

```
A:ALA-12>config>log# info
----------------------------------------------
...
event-control 2014 generate critical
...
----------------------------------------------
A:ALA-12>config>log#
```

Example: Command usage to modify event control

```
  config# log
 config>log# event-control 2014 suppress
```

Example: Log filter configuration output

```
A:ALA-12>config>log# info
----------------------------------------------
...
        event-control 2014 suppress
...
----------------------------------------------
A:ALA-12>config>log#
```

5.6.4.12 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 syntax to modify event control parameters.

```
config>log
        no event-control application-id [event-name |event-nunmber]
```

Example: Command usage to return to default values

```
 config# log
config>log# no event-control 2001
config>log# no event-control 2002
config>log# no event-control 2014
```

Example: Configuration output

```
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#
```

5.7 Log command reference

5.7.1 Command hierarchies

- Configuration commands
  - Event control commands
  - Accounting policy commands
  - File ID commands
  - Event filter commands
  - Log ID commands
  - SNMP trap group commands
  - Syslog commands

- Show commands
- Clear commands
- Tools dump commands

5.7.1.1 Configuration commands

5.7.1.1.1 Event control 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
```

5.7.1.1.2 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
```

5.7.1.1.3 File ID commands

```
config
    - log
        - [no] file-id log-file-id
            - description description-string
            - no description
            - location cflash-id | usb-flash-id [backup-cflash-id]
            - no location
            - rollover minutes [retention hours]
            - no rollover
```

5.7.1.1.4 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
```

5.7.1.1.5 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
```

5.7.1.1.6 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}]]
```

5.7.1.1.7 Syslog commands

```
config
    - log
        - [no] syslog syslog-id
            - address ip-address
            - no address
            - description description-string
            - no description
            - facility syslog-facility
            - no facility
            - level {emergency | alert | critical | error | warning | notice | info | debug}
            - no level
            - log-prefix log-prefix-string
            - no log-prefix
            - port port
            - no port
```

5.7.1.2 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]
```

5.7.1.3 Clear commands

```
clear
    - log log-id
```

5.7.1.4 Tools dump commands

```
tools
    - dump
        - accounting-policy [id] flash-write-count [clear]
```

Note:
See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about the **tools dump accounting-policy** command.

5.7.2 Command descriptions

- Configuration commands
- Show commands
- Clear commands

5.7.2.1 Configuration commands

- Generic commands
- Event control commands
- Log file commands
- Log filter commands
- Log filter entry commands
- Log filter entry match commands
- Syslog commands
- SNMP trap group commands
- Logging destination commands
- Accounting policy commands

5.7.2.1.1 Generic commands

description

Syntax

description *string*

no description

Context

config>log

config>log>file-id

config>log>log-id

config>log>filter

config>log>filter>entry

config>log>accounting-policy

config>log>syslog

config>log>snmp-trap-group

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command creates a text description stored in the configuration file for a configuration context. The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

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

Parameters

string

Specifies a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

shutdown

Syntax

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

Context

config>log

config>log>accounting-policy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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

When a *log-id* is shut down, no events are collected for the entity. This leads to the loss of event data.

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.

5.7.2.1.2 Event control commands

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies that a particular event or all events associated with an application are either generated or suppressed.

Events are generated by an application and contain an event number and description of the cause of the event. Each event has a default designation that 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 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. However, the generation of too many events may cause excessive overhead.

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

The **no** form of this command reverts the parameters to the default setting for events for the application or a specific event within the application. The *severity-level*, **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

Specifies the application whose events are affected by this event control filter.

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

event-name* | *event-number

Specifies the event number or short name, which can generate, suppress, or revert to default for a single event. 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.

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**.

severity-name

Specifies an ASCII string representing the severity level to associate with the specified generated events.

Values 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

Keyword to indicate that the specified events will not be logged. If the **suppress** keyword is not specified, the events are generated by default.

route-preference

Syntax

route-preference primary {**inband** | **outband**} **secondary** {**inband** | **outband** | **none**}

no route-preference

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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, the secondary routing preference will be attempted.

The **no** form of this 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.

5.7.2.1.3 Log file commands

file-id

Syntax

[**no**] **file-id** *log-file-id*

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

Commands in this context 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 to use as the destination for a log event message stream or accounting or 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 system creates the filenames for a log, as summarized in the following table.

Table 46: File names

File type	Filename
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, 2016)
  - *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
- the sequence number of the last event stored on the log is recorded, if the event log file was closed properly

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** or **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 this 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.

Parameters

log-file-id

Specifies the file identification number, expressed as a decimal integer.

Values 1 to 99

location

Syntax

location *cflash-id* | *usb-flash-id* [*backup-cflash-id*]

no location

Context

config>log>file-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies the primary location where the log or billing file will be created.

When creating files, the primary location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available, an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space becomes available, the alarm condition will be cleared.

The **no** form of this command reverts to default settings.

Default

log files are created on cf1: and accounting files are created on cf1:

Parameters

cflash-id

Specifies the primary location.

Values cf1: | uf1: (7210 SAS-S 1/10GE (standalone and standalone-VC))

cf1: | cf2: | uf1: (7210 SAS-Mxp, 7210 SAS-T, 7210 SAS-Sx 1/10GE (standalone and standalone-VC), and 7210 SAS-Sx 10/100GE)

cf1: |cf1-A: | cf1-B: | cf2: | cf2-A: | cf2-B: | uf1: | uf1-A: | uf1-B: (7210 SAS-R6 and 7210 SAS-R12)

usb-flash-id

Specifies the USB location.

Values cf1: | uf1: (7210 SAS-S 1/10GE (standalone and standalone-VC))

cf1: | cf2: | uf1: (7210 SAS-Mxp, 7210 SAS-T, 7210 SAS-Sx 1/10GE (standalone and standalone-VC), and 7210 SAS-Sx 10/100GE)

cf1: | cf1-A: | cf1-B: | cf2: | cf2-A: | cf2-B: | uf1: | uf1-A: | uf1-B: (7210 SAS-R6 and 7210 SAS-R12)

backup-cflash-id

Specify the backup location.

Values cf1: | uf1: (7210 SAS-S 1/10GE (standalone and standalone-VC))

cf1: | cf2: | uf1 (7210 SAS-Mxp, 7210 SAS-T, and 7210 SAS-Sx/S 1/10GE (standalone and standalone-VC))

cf1: | cf1-A: | cf1-B: | cf2: | cf2-A: | cf2-B: | uf1: | uf1-A: | uf1-B: (7210 SAS-R6 and 7210 SAS-R12)

rollover

Syntax

rollover *minutes* [**retention** *hours*]

no rollover

Context

config>log>file-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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

Specifies the rollover time, in minutes.

Values 5 to 10080

retention hours

Specifies the retention period in hours, expressed as a decimal integer. The retention time is based on the creation time of the file. The file becomes a candidate for removal when the creation datestamp + rollover time + retention time equals less than the current timestamp.

Default 12

Values 1 to 500

5.7.2.1.4 Log filter commands

filter

Syntax

[**no**] **filter** *filter-id*

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command enables the 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 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.

Changes made to an existing filter using any of the subcommands are immediately applied to the destinations where the filter is applied.

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

Parameters

filter-id

Specifies the filter ID uniquely identifies the filter.

Values 1 to 1001

default-action

Syntax

default-action {**drop** | **forward**}

no default-action

Context

config>log>filter

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command 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 this command reverts to the default value.

Default

default-action forward

Parameters

drop

Keyword to specify that the events that are not explicitly forwarded by an event filter match are dropped.

forward

Keyword to specify that the events that are not explicitly dropped by an event filter match are forwarded.

5.7.2.1.5 Log filter entry commands

action

Syntax

action {**drop** | **forward**}

no action

Context

config>log>filter>entry

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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.

When multiple action statements are entered, the last action will overwrite the previous actions.

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

Default

the action specified by the default-action command

Parameters

drop

Keyword to specify that packets matching the entry criteria will be dropped.

forward

Keyword to specify that packets matching the entry criteria will be forwarded.

entry

Syntax

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

Context

config>log>filter

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

Commands in this context 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 stops 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 this command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log IDs where the filter is applied.

Parameters

entry-id

Specifies the entry ID, which 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 to 999

5.7.2.1.6 Log filter entry match commands

match

Syntax

[**no**] **match**

Context

config>log>filter>entry

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

Commands in this context create or 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, all 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 this command removes the match criteria for the *entry-id*.

application

Syntax

application {**eq** | **neq**} *application-id*

no application

Context

config>log>filter>entry>match

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command adds a 7210 SAS application as an event filter match criterion.

A 7210 SAS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, services, and others. Only one application can be specified. The latest **application** command overwrites the previous command.

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

Default

no application

Parameters

eq | neq

The operator specifying the type of match. Valid operators are listed in the following table.

Table 47: Valid application operators

Operator	Notes
eq	equal to

Operator	Notes
neq	not equal to

application-id

Specifies the application name string.

Values chassis | debug | efm_oam | eth_cfm | ering | filter | igmp_snooping | ip | isis | lag | ldp | lldp | logger | mirror | mpls | ntp | oam | ospf | port | route_policy | rsvp | security | snmp | stp | svcmgr | system | user | vrtr

number

Syntax

number {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *event-id*

no number

Context

config>log>filter>entry>match

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command adds a 7210 SAS application event number as a match criterion.

The 7210 SAS 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 this command removes the event number as a match criterion.

Default

no event-number

Parameters

eq | neq | lt | lte | gt | gte

Keyword to configure the operator that specifies the type of match. Valid operators are listed in the following table.

Table 48: Valid operators

Operator	Notes
eq	equal to

Operator	Notes
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id

Specifies the event ID, expressed as a decimal integer.

Values 1 to 4294967295

router

Syntax

router {**eq** | **neq**} *router-instance* [**regexp**]

no router

Context

config>log>filter>entry>match

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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

Keyword to specify the type of string comparison to use to determine whether 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 this command removes the severity match criterion.

Default

no severity

Parameters

eq | neq | lt | lte | gt | gte

Keyword to configure the operator that specifies the type of match. Valid operators are listed in the following table.

Table 49: Valid operators

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

Specifies the ITU severity level name. The following table lists severity names and corresponding numbers per ITU standards M.3100 X.733 and X.21 severity levels.

Table 50: 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>entry>match

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 this command removes the subject match criterion.

Default

no subject

Parameters

eq | neq

Keyword to configure the operator that specifies the type of match. Valid operators are listed in the following table.

Table 51: Valid operators

Operator	Notes
eq	equal to
neg	not equal to

subject

Specifies a string used as the subject match criterion.

regexp

Keyword to specify the type of string comparison to use to determine whether 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.

5.7.2.1.7 Syslog commands

syslog

Syntax

[**no**] **syslog** *syslog-id*

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context 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 IDs 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.

Parameters

syslog-id

Specifies the syslog ID number for the syslog destination, expressed as a decimal integer.

Values 1 to 10

address

Syntax

address *ip-address*

no address

Context

config>log>syslog

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the syslog target host IP address.

Default

no address

Parameters

ip-address

Specifies 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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, 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 specific facility code.

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

Default

facility local7

Parameters

syslog-facility

Specifies the syslog facility name, which 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 in accordance with RFC 3164, *The BSD syslog Protocol*, are listed in the following table.

Table 52: Valid responses

Numerical code	Facility code
0	kernel
1	user

Numerical code	Facility code
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
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

log-prefix

Syntax

log-prefix *log-prefix-string*

no log-prefix

Context

config>log>syslog

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 this command removes the log prefix string.

Default

no log-prefix

Parameters

log-prefix-string

Specifies an alphanumeric string up to 32 characters. Spaces and colons cannot be used in the string.

level

Syntax

level *syslog-level*

no level

Context

config>log>syslog

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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. Severity levels are shown in Table 53: Threshold severity levels.

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 this command reverts to the default value.

Parameters

value

The threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

Table 53: Threshold severity levels

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command reverts to default value.

Default

no port

Parameters

port

Specifies the configured UDP port number used when sending syslog messages.

Values 0 to 65535

throttle-rate

Syntax

throttle-rate *events* [**interval** *seconds*]

no throttle-rate

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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. When 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 to 20000

Default 500

seconds

Specifies the number of seconds that an event throttling interval lasts.

Values 1 to 60

Default 1

5.7.2.1.8 SNMP trap group commands

snmp-trap-group

Syntax

[**no**] **snmp-trap-group** *log-id*

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure a group of SNMP trap receivers and their operational parameters for a specific *log-id*.

A group specifies the types of SNMP traps and specifies the log ID that will receive the group of SNMP traps. A trap group must be configured 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. When 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 this command deletes the SNMP trap group.

Parameters

log-id

Specifies 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 to 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command notifies 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 messages even if EFM OAM is enabled. That is, the generation of an SNMP dying gasp trap is mutually exclusive to the use of the EFM OAM dying gasp message.

By default, the system generates an EFM OAM dying gasp message to remain compatible with earlier version of the software releases. The user must explicitly configure the system to send an SNMP trap on loss of power to the node using this command.

Typically, SNMP traps are generated only if the user configures a log to direct the system log events to SNMP. For the SNMP dying gasp trap, it is not required to do so. The DSCP value used by an SNMP dying gasp packet is AF (Assured Forwarding class, value 22).

The **no** form of this command disables the generation of an SNMP trap message. It enables the generation of an EFM OAM dying gasp on access-uplink ports if EFM OAM is enabled on those ports. Generation of a SNMP dying gasp trap is disabled by default.

Note:

- The system IP address must be configured. The node uses it to generate 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 are looked up. Configuration of the route preference does not change this behavior (that is, the order of route lookup does not change).

Parameters

primary *trap-target-group-num*

Specifies the trap target group number for the primary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-group-num* must correspond to one of the SNMP trap group configurations under **config log snmp-trap-group** *trap-num*.

Values 1 to 100

primary *trap-target-name*

Specifies the trap target name, up to 28 characters, for the primary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-name* must correspond to one of the SNMP trap receiver targets configured under **config log snmp-trap-group** *trap-num* **trap-target** *target-name*.

secondary *trap-target-group-num*

Specifies the trap target group number for the secondary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-group-num* must correspond to one of the SNMP trap group configurations under **config log snmp-trap-group** *trap-num*.

Values 1 to 100

secondary *trap-target-name*

Specifies the trap target name, up to 28 characters, for the secondary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-name* must correspond to one of the SNMP trap receiver targets configured under **config log snmp-trap-group** *trap-num* **trap-target** *target-name*.

tertiary *trap-target-group-num*

Specifies the trap target group number for the tertiary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-group-num* must correspond to one of the SNMP trap group configurations under **config log snmp-trap-group** *trap-num*.

Values 1 to 100

tertiary *trap-target-name*

Specifies the trap target name, up to 28 characters, for the tertiary SNMP trap receiver to which the system will address the SNMP trap. The *trap-target-name* must correspond to one of the SNMP trap receiver targets configured under **config log snmp-trap-group** *trap-num* **trap-target** *target-name*.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command creates or edits 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 or remove a trap receiver from an snmp-trap-group. The operational parameters specified in the command include the following:

- IP address of the trap receiver
- 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.

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 this command removes the SNMP trap receiver from the SNMP trap group.

Parameters

name

Specifies the name of the trap target, up to 28 characters.

ip-address

Specifies 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

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, multiple ports must be configured.

Default 162

Values 1 to 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 correct 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 correct 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**.

The following preexisting conditions are checked before the *snmpv3SecurityName* is accepted.

- The username 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 *communityName* | *snmpv3SecurityName*

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 correct 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.

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.

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.

5.7.2.1.9 Logging destination commands

filter

Syntax

filter *filter-id*

no filter

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 this command removes the specified event filter from the *log-id*.

Default

no filter

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 to 1001

from

Syntax

from {[**main**] [**security**] [**change**] [**debug-trace**]}

no from

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures 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 this command removes all previously configured source streams.

Parameters

main

Keyword to instruct 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

Keyword to instruct 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

Keyword to 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

Keyword to instruct 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

Commands in this context configure destinations for event streams.

The **log-id** context is used to direct events, alarms and 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:
Log ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. Nokia strongly recommends not to alter the configuration for Log ID 99.

The **no** form of this command deletes the log destination ID from the configuration.

Parameters

log-id

Specifies the log ID number, expressed as a decimal integer.

Values 1 to 100

to console

Syntax

to console

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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, all entries are dropped.

The source of the data stream must be specified in the **from** command before 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 re-created.

to file

Syntax

to file *log-file-id*

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 before 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 re-created.

Parameters

log-file-id

Specifies to instruct 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 to 99

to memory

Syntax

to memory [*size*]

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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. When 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 before 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 re-created.

Parameters

size

Specifies the number of events that can be stored in the memory.

Default 100

Values 50 to 1024

to session

Syntax

to session

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 before 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 re-created.

to snmp

Syntax

to snmp [*size*]

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies 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 before 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 recreated.

Parameters

size

Specifies the number of events stored in this memory log.

Default 100

Values 50 to 1024

to syslog

Syntax

to syslog *syslog-id*

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies 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 before 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 recreated.

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 to 10

time-format

Syntax

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

Context

config>log>log-id

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default

utc

Parameters

local

Keyword to specify that timestamps are written in the system local time.

utc

Keyword to specify that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

5.7.2.1.10 Accounting policy commands

accounting-policy

Syntax

accounting-policy *policy-id*

no accounting-policy *policy-id*

Context

config>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command enables 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 subcommands, 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, network IP interfaces and SDPs. Any changes made to an existing policy, using any of the subcommands, will be applied immediately to all network ports, IP interfaces or SDPs where this policy is applied.

If no accounting policy is defined on a network port, network IP interface and SDP, accounting records will be produced in accordance with the default network policy as designated with the **default** command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

On the 7210 SAS, a total of 21 accounting records are available. There are five types of accounting policies:

- access
- access port
- network
- network interface

- SDP (not supported on platforms operating in access-uplink mode)

When creating accounting policies, one access, one access port, one network, one network interface, and one SDP accounting policy can be defined as default. If statistics collection is enabled on an accounting object and no accounting policy is applied, the respective default accounting policy is used. If no default policy is defined, no statistics are collected unless a specifically defined accounting policy is applied.

The **no** form of this 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.

Parameters

policy-id

Specifies the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 to 99

collection-interval

Syntax

collection-interval *minutes*

no collection-interval

Context

config>log>accounting-policy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the accounting collection interval.

Parameters

minutes

Specifies the interval between collections, in minutes.

Values 5 to 120 A range of only 1 to 4 is allowed when the record type is set to SAA.

default

Syntax

[**no**] **default**

Context

config>log>accounting-policy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.

If no accounting policy is defined on an access or network object, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

When creating accounting policies, one access, one access port, one network, one network interface, and one SDP accounting policy can be defined as default.

The record name must be specified before 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 this 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command adds the accounting record type to the accounting policy to be forwarded to the configured accounting file. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

To configure an accounting policy for SAPs, select the access type accounting records such as service-ingress-packets; for access ports, select access port type records, such as access-egress-packets; for network ports select network type records, such as network-egress-packets; for IP interfaces, select network interface type records, such as network-interface-ingress-packets; and for SDP and SDP bindings select SDP type records, such as complete-sdp-ingress-egress.

If the change required modifies the record from one type to another, the old record name must be removed using the **no** form of this command.

Only one record may be configured in a single accounting policy. For example, if an accounting-policy is configured with an **access-egress-octets** record, 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:
Collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of this command removes the record type from the policy.

Parameters

record-name

Specifies the accounting record name.

Output

The following output is an example of show accounting records for 7210 SAS platforms.

Sample output for 7210 SAS-Sx 10/100GE

```
*A:7210SAS>show>log# accounting-records

===============================================================
Accounting Policy Records
===============================================================
Record # Record Name                          Def. Interval
---------------------------------------------------------------
1        service-ingress-octets               5
2        service-egress-octets                5
3        service-ingress-packets              5
4        service-egress-packets               5
5        network-ingress-octets               15
6        network-egress-octets                15
7        network-ingress-packets              15
8        network-egress-packets               15
10       combined-service-ingress             5
11       combined-network-ing-egr-octets      15
13       complete-service-ingress-egress      5
14       combined-sdp-ingress-egress          5
15       complete-sdp-ingress-egress          5
32       saa                                  5
56       complete-pm                          5
101      network-interface-ingress-octets     15
102      network-interface-ingress-packets    15
103      combined-network-interface-ingress   15
104      access-egress-packets                5
105      access-egress-octets                 5
106      combined-access-egress               5
107      combined-network-egress              15
108      combined-service-egress              5
===============================================================
*A:7210SAS>show>log#
```

to

Syntax

to file *file-id*

Context

config>log>accounting-policy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

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

Parameters

file-id

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, it becomes active during the next collection interval.

Values 1 to 99

log-memory

Syntax

log-memory

[**no**] **log-memory**

Context

config>log>accounting-policy

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 are lost on a reboot (either due to loss of power or due to user action).

5.7.2.2 Show commands

accounting-policy

Syntax

accounting-policy [acct-*policy-id*] [**access** | **network**]

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays accounting policy information.

Parameters

policy-id

Specifies the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 to 99

access

Specifies to display only access accounting policies.

network

Specifies to display only network accounting policies.

Output

The following output is an example of accounting policy information, and Table 54: Output fields: accounting policy describes the output fields.

Sample output

```
*A:7210-SAS>show>log# accounting-policy
==============================

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
....
```

Table 54: Output fields: accounting policy

Label	Description
Policy ID	Displays 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 sdp — Indicates that the policy is meant to collect accounting stats for SDPs and spoke SDPs access port — Indicates that the policy is an access port accounting policy which can be used to collect accounting records only for access ports network interface — Indicates that the policy is an network Interface accounting policy which can be used to collect accounting records only for network IP interface 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

Label	Description
	Down — Indicates that the policy is administratively disabled
Oper State	Displays the operational state of the policy Up — Indicates that the policy is operationally up Down — Indicates that the policy is operationally down
Intvl	Displays the interval, in minutes, in which statistics are collected and written to their destination The default depends on the record name type
File ID	Displays the log destination
Record Name	Displays 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	Displays 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

accounting-records

Syntax

accounting-records

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays accounting policy record names.

Output

The following output is an example of accounting record information, and Table 55: Output fields: accounting records describes the output fields.

Sample output

```
*A:7210-SAS>show>log# accounting-records

===========================================================
Accounting Policy Records
===========================================================
Record # Record Name                        Def. Interval
-----------------------------------------------------------
1        service-ingress-octets             5
2        service-egress-octets              5
3        service-ingress-packets            5
4        service-egress-packets             5
5        network-ingress-octets             15
6        network-egress-octets              15
7        network-ingress-packets            15
8        network-egress-packets             15
10       combined-service-ingress           5
11       combined-network-ing-egr-octets    15
13       complete-service-ingress-egress    5
14       combined-sdp-ingress-egress        5
15       complete-sdp-ingress-egress        5
32       saa                                5
33       network-interface-ingress-octets   15
34       network-interface-ingress-packets  15
35       combined-network-interface-ingress 15
36       access-egress-packets              5
37       access-egress-octets               5
38       combined-access-egress             5
39       combined-network-egress            15
40       combined-service-egress            5
===========================================================
*A:7210-SAS>show>log#
```

Table 55: Output fields: accounting records

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

applications

Syntax

applications

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command displays a list of all application names that can be used in **event-control** and **filter** commands.

Output

The following output is an example of application name information.

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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

Displays event control for only the specified application.

Default all applications

Values chassis | debug | efm_oam | eth_cfm | ering | filter | igmp_snooping | ip | isis | lag | ldp | lldp | logger | mirror | mpls | ntp | oam | ospf | port | route_policy | rsvp | security | snmp | stp | svcmgr | system | user | vrtr

event-name

Displays event control only for the named application event.

Default all events for the application

event-number

Displays event control for only the specified application event number.

Default all events for the application

Values 0 to 4294967295

Output

The following output is an example of event control settings information, and Table 56: Output fields: event control describes the output fields.

Sample output

```
*A:SAS>show>log# event-control
===============================================================================
Log Events
===============================================================================
```

```
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
---------------------------------------------------------------------------
BGP:
   2001 bgpEstablished                    MI  gen          0           0
   2002 bgpBackwardTransition             WA  gen          0           0
   2003 tBgpMaxPrefix90                   WA  gen          0           0
   2004 tBgpMaxPrefix100                  CR  gen          0           0
L  2005 sendNotification                  WA  gen          0           0
L  2006 receiveNotification               WA  gen          0           0
L  2007 bgpInterfaceDown                  WA  gen          0           0
L  2008 bgpConnNoKA                       WA  gen          0           0
L  2009 bgpConnNoOpenRcvd                 WA  gen          0           0
L  2010 bgpRejectConnBadLocAddr           WA  gen          0           0
L  2011 bgpRemoteEndClosedConn            WA  gen          0           0
L  2012 bgpPeerNotFound                   WA  gen          0           0
L  2013 bgpConnMgrTerminated              WA  gen          0           0
L  2014 bgpTerminated                     WA  gen          0           0
L  2015 bgpNoMemoryPeer                   CR  gen          0           0
L  2016 bgpVariableRangeViolation         WA  gen          0           0
L  2017 bgpCfgViol                        WA  gen          0           0
   2018 tBgpPeerGRStatusChange            WA  gen          0           0
   2019 tBgpNgEstablished                 MI  gen          0           0
   2020 tBgpNgBackwardTransition          WA  gen          0           0
   2021 tBgpPeerNgHoldTimeInconsistent    WA  gen          0           0
CHASSIS:
   2001 cardFailure                       MA  gen          0           0
   2002 cardInserted                      MI  gen          5           0
   2003 cardRemoved                       MI  gen          0           0
   2004 cardWrong                         MI  gen          0           0
   2005 EnvTemperatureTooHigh             MA  gen          0           0
   2006 fanFailure                        CR  gen          0           0
   2007 powerSupplyOverTemp               CR  gen          0           0
   2008 powerSupplyAcFailure              CR  gen          0           0
   2009 powerSupplyDcFailure              CR  gen          0           0
   2010 powerSupplyInserted               MA  gen          1           0
   2011 powerSupplyRemoved                MA  gen          0           0
   2012 redPrimaryCPMFail                 CR  gen          0           0
   2016 clearNotification                 MA  gen          0           0
   2017 syncIfTimingHoldover              CR  gen          0           0
   2018 syncIfTimingHoldoverClear         CR  gen          0           0
   2019 syncIfTimingRef1Alarm             MI  gen          0           0
   2020 syncIfTimingRef1AlarmClear        MI  gen          0           0
   2021 syncIfTimingRef2Alarm             MI  gen          0           0
   2022 syncIfTimingRef2AlarmClear        MI  gen          0           0
   2023 flashDataLoss                     MA  gen          0           0
   2024 flashDiskFull                     MA  gen          0           0
   2025 softwareMismatch                  MA  gen          0           0
   2026 softwareLoadFailed                MA  gen          0           0
   2027 bootloaderMismatch                MA  gen          1           0
   2028 bootromMismatch                   MA  gen          0           0
   2029 fpgaMismatch                      MA  gen          0           0
   2030 syncIfTimingBITSAlarm             MI  gen          0           0
   2031 syncIfTimingBITSAlarmClear        MI  gen          0           0
   2032 cardUpgraded                      MA  gen          0           0
   2033 cardUpgradeInProgress             MA  gen          0           0
   2034 cardUpgradeComplete               MA  gen          0           0
   2050 powerSupplyInputFailure           CR  gen          0           0
   2051 powerSupplyOutputFailure          CR  gen          0           0
   2052 mdaHiBwMulticastAlarm             MI  gen          0           0
   2056 mdaCfgNotCompatible               MA  gen          0           0
   2057 cardSyncFileNotPresent            MI  gen          0           0
   2058 tmnxEqMdaXplError                 MI  sup          0           0
   2059 tmnxEqCardPChipError              MI  sup          0           0
```

```
   2060 tmnxEqCardSoftResetAlarm          MI  gen          0          0
   2061 tmnxEqMdaSyncENotCompatible       MA  gen          0          0
   2062 tmnxIPsecIsaGrpActiveIsaChgd      MI  gen          0          0
   2063 tmnxEqCardPChipMemoryEvent        MI  sup          0          0
   2064 tmnxIPsecIsaGrpUnableToSwitch     MI  gen          0          0
   2065 tmnxIPsecIsaGrpTnlLowWMark        MI  gen          0          0
   2066 tmnxIPsecIsaGrpTnlHighWMark       MI  gen          0          0
   2067 tmnxIPsecIsaGrpTnlMax             MI  gen          0          0
   2076 tmnxEqCardPChipCamEvent           CR  gen          0          0
   2078 tmnxEqHwEnhancedCapability        MA  gen          0          0
   2068 tmnxEqSyncIfTimingRef1Quality     MI  gen          0          0
   2069 tmnxEqSyncIfTimingRef2Quality     MI  gen          0          0
   2072 tmnxEqSyncIfTimingRefSwitch       MI  gen          0          0
   2077 tmnxEqSyncIfTimingSystemQuality   MI  gen          1          0
   3001 tmnxSasAlarminput1StateChanged    MA  gen          0          0
   3002 tmnxSasAlarminput2StateChanged    MA  gen          0          0
   3003 tmnxSasAlarminput3StateChanged    MA  gen          0          0
   3004 tmnxSasAlarminput4StateChanged    MA  gen          0          0
   3000 EnvTemperatureTooLow              MA  gen          0          0
DEBUG:
L  2001 traceEvent                        MI  gen          0          0
EFM_OAM:
   2001 tmnxDot3OamPeerChanged            MI  gen          0          0
   2002 tmnxDot3OamLoopDetected           MI  gen          0          0
   2003 tmnxDot3OamLoopCleared            MI  gen          0          0
   2008 dot3OamNonThresholdEvent          MI  gen          0          0
   2902 tmnxDyingGasp                     MI  gen          0          0
ETH_CFM:
   2001 dot1agCfmFaultAlarm               MI  gen          0          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          0          0
   2007 tmnxDot1agCfmMipEvaluation        MI  gen          0          0
ERING:
   2001 tmnxEthRingPathFwdStateChange     MI  gen          0          0
   2002 tmnxEthRingApsPrvsnRaiseAlarm     MI  gen          0          0
   2003 tmnxEthRingApsPrvsnClearAlarm     MI  gen          0          0
ETUN:
   2001 tmnxEthTunnelApsCfgRaiseAlarm     MI  gen          0          0
   2002 tmnxEthTunnelApsCfgClearAlarm     MI  gen          0          0
   2003 tmnxEthTunnelApsPrvsnRaiseAlarm   MI  gen          0          0
   2004 tmnxEthTunnelApsPrvsnClearAlarm   MI  gen          0          0
   2005 tmnxEthTunnelApsNoRspRaiseAlarm   MI  gen          0          0
   2006 tmnxEthTunnelApsNoRspClearAlarm   MI  gen          0          0
   2007 tmnxEthTunnelApsSwitchoverAlarm   MI  gen          0          0
FILTER:
   2001 tIPFilterPBRPacketsDrop           WA  gen          0          0
   2002 tFilterEntryActivationFailed      WA  gen          0          0
   2003 tFilterEntryActivationRestored    WA  gen          0          0
IGMP_SNOOPING:
   2001 sapIgmpSnpgGrpLimitExceeded       WA  gen          0          0
   2002 sapIgmpSnpgMcacPlcyDropped        WA  gen          0          0
   2003 sdpBndIgmpSnpgGrpLimitExceeded    WA  gen          0          0
   2004 sdpBndIgmpSnpgMcacPlcyDropped     WA  gen          0          0
   2005 sapIgmpSnpgMcsFailure             WA  gen          0          0
   2006 sapIgmpSnpgSrcLimitExceeded       WA  gen          0          0
   2007 sdpBndIgmpSnpgSrcLimitExceeded    WA  gen          0          0
IP:
L  2001 clearRTMError                     MI  gen          0          0
L  2002 ipEtherBroadcast                  MI  gen          0          0
L  2003 ipDuplicateAddress                MI  gen          0          0
L  2004 ipArpInfoOverwritten              MI  gen          0          0
```

```
L  2005 fibAddFailed                       MA  gen          0          0
L  2006 qosNetworkPolicyMallocFailed       MA  gen          0          0
L  2007 ipArpBadInterface                  MI  gen          0          0
L  2008 ipArpDuplicateIpAddress            MI  gen          0          0
L  2009 ipArpDuplicateMacAddress           MI  gen          0          0
L  2010 ipAnyDuplicateAddress              MI  gen          0          0
ISIS:
   2001 vRtrIsisDatabaseOverload           WA  gen          0          0
   2002 vRtrIsisManualAddressDrops         WA  gen          0          0
   2003 vRtrIsisCorruptedLSPDetected       WA  gen          0          0
   2004 vRtrIsisMaxSeqExceedAttempt        WA  gen          0          0
   2005 vRtrIsisIDLenMismatch              WA  gen          0          0
   2006 vRtrIsisMaxAreaAddrsMismatch       WA  gen          0          0
   2007 vRtrIsisOwnLSPPurge                WA  gen          0          0
   2008 vRtrIsisSequenceNumberSkip         WA  gen          0          0
   2009 vRtrIsisAutTypeFail                WA  gen          0          0
   2010 vRtrIsisAuthFail                   WA  gen          0          0
   2011 vRtrIsisVersionSkew                WA  gen          0          0
   2012 vRtrIsisAreaMismatch               WA  gen          0          0
   2013 vRtrIsisRejectedAdjacency          WA  gen          0          0
   2014 vRtrIsisLSPTooLargeToPropagate     WA  gen          0          0
   2015 vRtrIsisOrigLSPBufSizeMismatch     WA  gen          0          0
   2016 vRtrIsisProtoSuppMismatch          WA  gen          0          0
   2017 vRtrIsisAdjacencyChange            WA  gen          0          0
   2018 vRtrIsisCircIdExhausted            WA  gen          0          0
   2019 vRtrIsisAdjRestartStatusChange     WA  gen          0          0
   2020 vRtrIsisLdpSyncTimerStarted        WA  gen          0          0
   2021 vRtrIsisLdpSyncExit                WA  gen          0          0
LAG:
   2001 DynamicCostOn                      WA  gen          0          0
   2002 DynamicCostOff                     WA  gen          0          0
   2003 LagPortAddFailed                   WA  gen          0          0
   2004 LagSubGroupSelected                WA  gen          0          0
   2005 LagPortAddFailureCleared           WA  gen          0          0

LDP:
   2001 vRtrLdpStateChange                 MI  gen          0          0
   2002 vRtrLdpInstanceStateChange         MI  gen          0          0
   2003 vRtrLdpIfStateChange               MI  sup          0          0
   2004 vRtrLdpGroupIdMismatch             MI  gen          0          0
LLDP:
   2001 lldpRemTablesChange                MI  gen          0          0
LOGGER:
L  2001 STARTED                            MI  gen          5          0
   2002 tmnxLogTraceError                  CR  gen          0          0
   2005 tmnxLogSpaceContention             MA  gen          0          0
   2006 tmnxLogAdminLocFailed              MA  gen          0          0
   2007 tmnxLogBackupLocFailed             MA  gen          0          0
   2008 tmnxLogFileRollover                MA  gen          0          0
   2009 tmnxLogFileDeleted                 MI  gen          0          0
   2010 tmnxClear                          IN  gen          0          0
   2011 tmnxTestEvent                      IN  gen          0          0
   2012 tmnxLogEventThrottled              MA  gen          0          0
   2013 tmnxSysLogTargetProblem            MA  gen          0          0
   2014 tmnxLogAccountingDataLoss          MA  gen          0          0
   2015 tmnxStdEventsReplayed              MA  gen          0          0
L  2016 tmnxLogOnlyEventThrottled          MA  gen          0          0
MC_REDUNDANCY:
   2001 tmnxMcRedundancyPeerStateChanged WA  gen          0          0
   2002 tmnxMcRedundancyMismatchDetected WA  gen          0          0
   2003 tmnxMcRedundancyMismatchResolved WA  gen          0          0
   2004 tmnxMcPeerSyncStatusChanged       WA  gen          0          0
   2005 tmnxMcSyncClientAlarmRaised       WA  gen          0          0
   2006 tmnxMcSyncClientAlarmCleared      WA  gen          0          0
```

```
   2007 tmnxSrrpSubnetMismatch           WA  gen          0          0
   2008 tmnxSrrpSubnetMismatchCleared    WA  gen          0          0
   2009 tmnxSrrpInstanceIdMismatch       WA  gen          0          0
   2010 tmnxSrrpSapMismatch              WA  gen          0          0
   2011 tmnxSrrpSapTagMismatch           WA  gen          0          0
   2012 tmnxSrrpRedIfMismatch            WA  gen          0          0
   2013 tmnxSrrpDualMaster               WA  gen          0          0
   2014 tmnxMcLagInfoLagChanged          WA  gen          0          0
   2015 tmnxSrrpSystemIpNotSet           WA  gen          0          0
   2016 tmnxMcRingOperStateChanged       WA  gen          0          0
   2017 tmnxMcRingInbCtrlOperStateChgd   WA  gen          0          0
   2018 tmnxMcRingNodeLocOperStateChgd   WA  gen          0          0
   2019 tmnxMcSyncClockSkewRaised        WA  gen          0          0
   2020 tmnxMcSyncClockSkewCleared       WA  gen          0          0
   2021 tmnxSrrpDuplicateSubIfAddress    WA  gen          0          0
   2022 tmnxMcPeerRingsOperStateChanged  WA  gen          0          0
   2023 tmnxSrrpTrapNewMaster            MI  gen          0          0
   2024 tmnxSrrpBecameBackup             MI  gen          0          0
L  2025 srrpPacketDiscarded              MI  gen          0          0
   2026 tmnxSrrpBfdIntfSessStateChgd     MI  gen          0          0
   2027 tmnxMcPeerEPBfdSessionOpen       WA  gen          0          0
   2028 tmnxMcPeerEPBfdSessionClose      WA  gen          0          0
   2029 tmnxMcPeerEPBfdSessionUp         WA  gen          0          0
   2030 tmnxMcPeerEPBfdSessionDown       WA  gen          0          0
   2031 tmnxMcPeerEPOperDown             WA  gen          0          0
   2032 tmnxMcPeerEPOperUp               WA  gen          0          0
   2033 tmnxMCEPSessionPsvModeEnabled    WA  gen          0          0
   2034 tmnxMCEPSessionPsvModeDisabled   WA  gen          0          0
MIRROR:
   2001 sourceEnabled                    MI  gen          0          0
   2002 sourceDisabled                   MI  gen          0          0
   2003 destinationEnabled               MI  gen          0          0
   2004 destinationDisabled              MI  gen          0          0
   2006 sourceIpFilterChange             MI  gen          0          0
   2007 sourceMacFilterChange            MI  gen          0          0
   2008 sourceSapChange                  MI  gen          0          0
   2009 sourceSubscriberChange           MI  gen          0          0
MPLS:
   2001 mplsXCUp                         WA  gen          0          0
   2002 mplsXCDown                       WA  gen          0          0
   2003 mplsTunnelUp                     WA  gen          0          0
   2004 mplsTunnelDown                   WA  gen          0          0
   2005 mplsTunnelRerouted               WA  sup          0          0
   2006 mplsTunnelReoptimized            WA  sup          0          0
   2007 vRtrMplsStateChange              WA  gen          0          0
   2008 vRtrMplsIfStateChange            WA  gen          0          0
   2009 vRtrMplsLspUp                    WA  gen          0          0
   2010 vRtrMplsLspDown                  WA  gen          0          0
   2011 vRtrMplsLspPathUp                WA  gen          0          0
   2012 vRtrMplsLspPathDown              WA  gen          0          0
   2013 vRtrMplsLspPathRerouted          WA  gen          0          0
   2014 vRtrMplsLspPathResignaled        WA  gen          0          0
   2015 vRtrMplsP2mpInstanceUp           WA  gen          0          0
   2016 vRtrMplsP2mpInstanceDown         WA  gen          0          0
   2017 vRtrMplsS2lSubLspUp              WA  gen          0          0
   2018 vRtrMplsS2lSubLspDown            WA  gen          0          0
   2019 vRtrMplsS2lSubLspRerouted        WA  gen          0          0
   2020 vRtrMplsS2lSubLspResignaled      WA  gen          0          0
   2021 vRtrMplsLspPathSoftPreempted     WA  gen          0          0
   2022 vRtrMplsLspPathLstFillReoptElig  WA  gen          0          0
   2023 vRtrMplsP2mpInstanceResignaled   WA  gen          0          0
   2024 vRtrMplsResignalTimerExpired     WA  gen          0          0
NTP:
   2001 tmnxNtpAuthMismatch              WA  gen          0          0
```

```
   2002 tmnxNtpNoServersAvail            MA  gen          0          0
   2003 tmnxNtpServersAvail              MI  gen          0          0
   2008 tmnxNtpOperChange                WA  gen          0          0
   2009 tmnxNtpServerChange              MI  gen          0          0
OAM:
   2001 tmnxOamPingProbeFailedV3         MI  gen          0          0
   2002 tmnxOamPingTestFailedV3          MI  gen          0          0
   2003 tmnxOamPingTestCompletedV3       MI  gen          0          0
   2004 tmnxAncpLoopbackTestCompleted    WA  gen          0          0
L  2005 tmnxAncpLoopbackTestCompletedL   WA  gen          0          0
   2050 tmnxOamTrPathChange              MI  gen          0          0
   2051 tmnxOamTrTestFailed              MI  gen          0          0
   2052 tmnxOamTrTestCompleted           MI  gen          0          0
L  2053 svcIdInvalid                     MI  gen          0          0
L  2054 svcIdWrongType                   MI  gen          0          0
   2055 tmnxOamLdpTtraceAutoDiscState    MI  gen          0          0
   2056 tmnxOamLdpTtraceFecProbeState    MI  gen          0          0
   2057 tmnxOamLdpTtraceFecDisStatus     MI  gen          0          0
   2101 tmnxOamSaaThreshold              MI  gen          0          0
OSPF:
   2001 tmnxOspfVirtIfStateChange        WA  gen          0          0
   2002 tmnxOspfNbrStateChange           WA  gen          0          0
   2003 tmnxOspfVirtNbrStateChange       WA  gen          0          0
   2004 tmnxOspfIfConfigError            WA  gen          0          0
   2005 tmnxOspfVirtIfConfigError        WA  gen          0          0
   2006 tmnxOspfIfAuthFailure            WA  gen          0          0
   2007 tmnxOspfVirtIfAuthFailure        WA  gen          0          0
   2008 tmnxOspfIfRxBadPacket            WA  gen          0          0
   2009 tmnxOspfVirtIfRxBadPacket        WA  gen          0          0
   2010 tmnxOspfTxRetransmit             WA  sup          0          0
   2011 tmnxOspfVirtIfTxRetransmit       WA  sup          0          0
   2012 tmnxOspfAreaOriginateLsa         WA  sup          0          0
   2013 tmnxOspfAreaMaxAgeLsa            WA  gen          0          0
   2014 tmnxOspfLsdbOverflow             WA  gen          0          0
   2015 tmnxOspfLsdbApproachingOverflow  WA  gen          0          0
   2016 tmnxOspfIfStateChange            WA  gen          0          0
   2017 tmnxOspfNssaTranslatorStatusChg  WA  gen          0          0
   2018 tmnxOspfRestartStatusChange      WA  gen          0          0
   2019 tmnxOspfNbrRestartHlprStsChg     WA  gen          0          0
   2020 tmnxOspfVirtNbrRestartHlprStsChg WA  gen          0          0
   2021 tmnxOspfSpfRunsStopped           WA  gen          0          0
   2022 tmnxOspfSpfRunsRestarted         WA  gen          0          0
   2023 tmnxOspfOverloadEntered          WA  gen          0          0
   2024 tmnxOspfOverloadExited           WA  gen          0          0
   2025 tmnxOspfAsOriginateLsa           WA  sup          0          0
   2026 tmnxOspfAsMaxAgeLsa              WA  gen          0          0
   2027 tmnxOspfLinkOriginateLsa         WA  sup          0          0
   2028 tmnxOspfLinkMaxAgeLsa            WA  gen          0          0
   2029 tmnxOspfLdpSyncTimerStarted      WA  gen          0          0
   2030 tmnxOspfLdpSyncExit              WA  gen          0          0
   2031 tmnxOspfShamIfStateChange        WA  gen          0          0
   2032 tmnxOspfShamNbrStateChange       WA  gen          0          0
   2033 tmnxOspfShamIfConfigError        WA  gen          0          0
   2034 tmnxOspfShamIfAuthFailure        WA  gen          0          0
   2035 tmnxOspfShamIfRxBadPacket        WA  gen          0          0
   2036 tmnxOspfShamIfTxRetransmit       WA  gen          0          0
   2037 tmnxOspfShamNbrRestartHlprStsChg WA  gen          0          0
   2038 tmnxOspfFailureDisabled          WA  gen          0          0
PORT:
   2001 sonetSDHAlarmSet                 MI  gen          0          0
   2002 sonetSDHAlarmClear               MI  gen          0          0
   2003 sonetSDHChannelAlarmSet          MI  gen          0          0
   2004 sonetSDHChannelAlarmClear        MI  gen          0          0
   2005 SFPInserted                      MI  gen         17          0
```

```
   2006 SFPRemoved                          MI  gen          3           0
   2008 SFPStatusFailure                    MI  gen          0           0
   2009 portError                           MI  gen          0           0
   2010 yellowDiffDelayExceeded             MI  gen          0           0
   2011 redDiffDelayExceeded                MA  gen          0           0
   2012 bndlBadEndPtDiscriminator           MI  gen          0           0
   2013 ds3AlarmSet                         MI  gen          0           0
   2014 ds3AlarmClear                       MI  gen          0           0
   2015 ds1AlarmSet                         MI  gen          0           0
   2016 ds1AlarmClear                       MI  gen          0           0
   2017 etherAlarmSet                       MI  gen          5           0
   2018 etherAlarmClear                     MI  gen          4           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          9           0
   2031 SFPStatusDDMCorrupt                 MI  gen          0           0
   2032 SFPStatusReadError                  MI  gen          0           0
   2033 SFPStatusUnsupported                MI  gen          0           0
   2034 dsxClockSyncStateChange             MI  gen          0           0
   2035 bundleMlfrMemberLoopback            MI  gen          0           0
   2036 tmnxPortUnsupportedFunction         WA  gen          0           0
   2037 otuAlarms                           MI  gen          0           0
ROUTE_POLICY:
L  2001 trigPolicyPrevEval                  WA  gen          0           0
RSVP:
   2001 vRtrRsvpStateChange                 WA  gen          0           0
   2002 vRtrRsvpIfStateChange               WA  gen          0           0
   2003 vRtrRsvpIfNbrStateUp                WA  gen          0           0
   2004 vRtrRsvpIfNbrStateDown              WA  gen          0           0
SECURITY:
L  2001 cli_user_login                      MI  gen          3           0
L  2002 cli_user_logout                     MI  gen          2           0
L  2003 cli_user_login_failed               MI  gen          0           0
L  2004 cli_user_login_max_attempts         MI  gen          0           0
L  2005 ftp_user_login                      MI  gen          0           0
L  2006 ftp_user_logout                     MI  gen          0           0
L  2007 ftp_user_login_failed               MI  gen          0           0
L  2008 ftp_user_login_max_attempts         MI  gen          0           0
L  2009 ssh_user_login                      MI  gen          0           0
L  2010 ssh_user_logout                     MI  gen          0           0
L  2011 ssh_user_login_failed               MI  gen          0           0
L  2012 ssh_user_login_max_attempts         MI  gen          0           0
   2014 radiusOperStatusChange              MI  gen          0           0
L  2015 user_disconnect                     MA  gen          0           0
L  2016 radiusSystemIpAddrNotSet            MA  gen          0           0
   2018 tacplusOperStatusChange             MI  gen          0           0
L  2019 mafEntryMatch                       MA  gen          0           0
L  2020 ftp_transfer_successful             MI  gen          0           0
L  2021 ftp_transfer_failed                 MI  gen          0           0
L  2022 enable_admin                        WA  gen          0           0
L  2023 host_snmp_attempts                  WA  gen          0           0
   2024 SSH_server_preserve_key_fail        MI  gen          0           0
   2025 tacplusInetSrvrOperStatusChange     MI  gen          0           0
   2026 radiusInetServerOperStatusChange    MI  gen          0           0
   2027 tmnxKeyChainAuthFailure             MI  gen          0           0
```

```
   2028 tmnxCpmProtViolPort               WA  gen          0          0
   2029 tmnxCpmProtViolPortAgg            WA  gen          0          0
   2030 tmnxCpmProtViolIf                 WA  gen          0          0
   2031 tmnxCpmProtViolSap                WA  gen          0          0
   2032 tmnxCpmProtViolMac                WA  gen          0          0
   2033 tmnxCpmProtViolVdoSvcClient       WA  gen          0          0
   2034 tmnxCpmProtViolVdoVrtrClient      WA  gen          0          0
   2206 tmnxConfigModify                  WA  gen          2          0
   2207 tmnxConfigCreate                  WA  gen          2          0
   2208 tmnxConfigDelete                  WA  gen          0          0
   2209 tmnxStateChange                   WA  gen          0          0
SNMP:
   2001 coldStart                         MA  gen          1          0
   2002 warmStart                         MA  gen          0          0
   2003 authenticationFailure             MI  sup          0          0
   2004 linkDown                          WA  gen          5          0
   2005 linkUp                            WA  gen          8          0
   2101 risingAlarm                       MA  gen          0          0
   2102 fallingAlarm                      MA  gen          0          0
   2201 snmpdError                        MA  gen          0          0
STP:
   2001 topologyChangeSapMajorState       WA  gen          0          0
   2002 newRootSap                        WA  gen          0          0
   2003 topologyChangeVcpState            WA  gen          0          0
   2004 newRootVcpState                   WA  gen          0          0
   2005 topologyChangeSapState            WA  gen          0          0
   2006 receivedTCN                       WA  gen          0          0
   2007 newRootBridge                     WA  gen          0          0
   2008 unacknowledgedTCN                 WA  gen          0          0
   2009 higherPriorityBridge              WA  gen          0          0
   2011 sapEncapPVST                      MI  gen          0          0
   2012 sapEncapDot1d                     MI  gen          0          0
   2014 tmnxSvcTopoChgSdpBindMajorState   WA  gen          0          0
   2015 tmnxSvcNewRootSdpBind             WA  gen          0          0
   2016 tmnxSvcTopoChgSdpBindState        WA  gen          0          0
   2017 tmnxSvcSdpBindRcvdTCN             WA  gen          0          0
   2018 tmnxSvcSdpBindRcvdHigherBriPrio   WA  gen          0          0
   2019 tmnxSvcSdpBindEncapPVST           MI  gen          0          0
   2020 tmnxSvcSdpBindEncapDot1d          MI  gen          0          0
   2021 tmnxNewCistRegionalRootBridge     WA  gen          0          0
   2022 tmnxNewMstiRegionalRootBridge     WA  gen          0          0
   2023 tmnxStpRootGuardViolation         WA  gen          0          0
   2024 tmnxStpMeshNotInMstRegion         WA  gen          0          0
   2025 tmnxSapStpExcepCondStateChng      WA  gen          0          0
   2026 tmnxSdpBndStpExcepCondStateChng   WA  gen          0          0
   2050 sapActiveProtocolChange           MI  gen          0          0
   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          4          0
   2104 svcTlsFdbTableFullAlarmRaised     MI  gen          0          0
   2105 svcTlsFdbTableFullAlarmCleared    MI  gen          0          0
   2108 iesIfStatusChanged                MI  gen          0          0
   2109 tmnxSvcObjTodSuiteApplicFailed    WA  gen          0          0
   2110 tmnxEndPointTxActiveChanged       WA  gen          0          0
   2111 tmnxSvcPEDiscPolServOperStatChg   MI  gen          0          0
   2120 svcTlsMrpAttrRegistrationFailed   MI  gen          0          0
   2125 svcTlsMrpAttrTblFullAlarmRaised   MI  gen          0          0
   2126 svcTlsMrpAttrTblFullAlarmCleared  MI  gen          0          0
```

```
   2128 svcEpipePbbOperStatusChanged     MI  gen          0          0
   2203 sapStatusChanged                 MI  gen          2          0
   2204 sapTlsMacAddrLimitAlarmRaised    MI  gen          0          0
   2205 sapTlsMacAddrLimitAlarmCleared   MI  gen          0          0
   2206 hostConnectivityLost             WA  gen          0          0
   2207 hostConnectivityRestored         WA  gen          0          0
   2208 sapReceivedProtSrcMac            MI  gen          0          0
   2209 sapTlsMacMoveExceeded            MI  gen          0          0
   2210 sapPortStateChangeProcessed      MA  gen          0          0
   2211 sapCemPacketDefectAlarm          MI  gen          0          0
   2212 sapCemPacketDefectAlarmClear     MI  gen          0          0
   2213 msapStateChanged                 MI  gen          0          0
   2214 msapCreationFailure              MI  gen          0          0
   2303 sdpStatusChanged                 MI  gen          0          0
   2306 sdpBindStatusChanged             MI  gen          0          0
L  2307 sdpKeepAliveStarted              MI  gen          0          0
L  2308 sdpKeepAliveStopped              MI  gen          0          0
L  2309 sdpKeepAliveProbeFailure         MI  gen          0          0
L  2310 sdpKeepAliveLateReply            MI  gen          0          0
   2311 sdpTlsMacAddrLimitAlarmRaised    MI  gen          0          0
   2312 sdpTlsMacAddrLimitAlarmCleared   MI  gen          0          0
   2313 sdpBindPwPeerStatusBitsChanged   MI  gen          0          0
   2314 sdpBindTlsMacMoveExceeded        MI  gen          0          0
   2315 sdpBindPwPeerFaultAddrChanged    MI  gen          0          0
   2316 sdpBindSdpStateChangeProcessed   MA  gen          0          0
   2317 sdpBandwidthOverbooked           MA  gen          0          0
   2318 sdpBindInsufficientBandwidth     MA  gen          0          0
   2319 dynamicSdpConfigChanged          MA  gen          0          0
   2320 dynamicSdpBindConfigChanged      MA  gen          0          0
   2321 dynamicSdpCreationFailed         MA  gen          0          0
   2322 dynamicSdpBindCreationFailed     MA  gen          0          0
   2401 svcTlsMfibTableFullAlarmRaised   MI  gen          0          0
   2402 svcTlsMfibTableFullAlarmCleared  MI  gen          0          0
   2500 tmnxSubscriberCreated            WA  gen          0          0
   2501 tmnxSubscriberDeleted            WA  gen          0          0
   2502 tmnxSubscriberRenamed            WA  gen          0          0
   2503 tmnxSubAcctPlcyFailure           WA  gen          0          0
   2504 tmnxSubMcsRelatedProblem         WA  gen          0          0
   2505 tmnxSubAuthPlcyRadSerOperStatChg MI  gen          0          0
   2506 tmnxSubAcctPlcyRadSerOperStatChg MI  gen          0          0
   2507 svcEndPointMacLimitAlarmRaised   MI  gen          0          0
   2508 svcEndPointMacLimitAlarmCleared  MI  gen          0          0
   2509 tmnxSubRadSapDisconnectError     WA  gen          0          0
   2510 tmnxSubRadSdpBndDisconnectError  WA  gen          0          0
   2511 tmnxSubRadSapCoAError            WA  gen          0          0
   2512 tmnxSubRadSdpBndCoAError         WA  gen          0          0
   2513 tmnxSubRadSapSubAuthError        WA  gen          0          0
   2514 tmnxSubRadSdpBndSubAuthError     WA  gen          0          0
   2515 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         66           0
    2007 tmnxConfigCreate                 WA  gen         11           0
    2008 tmnxConfigDelete                 WA  gen          0           0
    2009 tmnxStateChange                  WA  gen          7           0
    2010 tmnxModuleMallocFailed           MA  gen          0           0
    2011 tmnxTrapDropped                  MA  gen          0           0
    2012 ssiSyncConfigOK                  WA  gen          0           0
    2013 ssiSyncConfigFailed              CR  gen          0           0
    2014 ssiSyncBootEnvOK                 WA  gen          0           0
    2015 ssiSyncBootEnvFailed             CR  gen          0           0
L   2016 socket_bind_failed              CR  gen          0           0
L   2017 socket_conn_accept_failed       CR  gen          0           0
    2018 sntpTimeDiffExceedsThreshold     MA  gen          0           0
    2022 tmnxSssiMismatch                 MA  gen          0           0
    2023 tmnxSnmpdStateChange             MA  gen          1           0
    2024 tmnxRedStandbySyncing            MA  gen          0           0
    2025 tmnxRedStandbyReady              MA  gen          0           0
    2026 tmnxRedStandbySyncLost           CR  gen          0           0
    2027 tmnxRedSwitchover                CR  gen          0           0
    2028 tmnxRedCpmActive                 CR  gen          0           0
    2029 tmnxRedSingleCpm                 CR  gen          0           0
    2030 persistencyClosedAlarmRaised     MA  gen          0           0
    2031 persistencyClosedAlarmCleared    MA  gen          0           0
    2032 tmnxSntpOperChange               MA  gen          0           0
    2034 tmnxFtpClientFailure             MI  gen          0           0
    2037 persistencyEventReport           WA  gen          0           0
    2038 sbiBootConfigFailFileError       MA  gen          0           0
    2039 sbiBootConfigOKFileError         MA  gen          0           0
    2101 schedActionFailure               MA  gen          0           0
    2102 smScriptAbort                    MA  gen          0           0
    2103 smScriptResult                   MI  sup          0           0
    2104 smScriptException                MI  sup          0           0
USER:
L   2001 cli_user_login                   MI  gen          3           0
L   2002 cli_user_logout                  MI  gen          2           0
L   2003 cli_user_login_failed            MI  gen          0           0
L   2004 cli_user_login_max_attempts      MI  gen          0           0
L   2005 ftp_user_login                   MI  gen          0           0
L   2006 ftp_user_logout                  MI  gen          0           0
L   2007 ftp_user_login_failed            MI  gen          0           0
L   2008 ftp_user_login_max_attempts      MI  gen          0           0
L   2009 cli_user_io                      MI  sup          0          35
L   2010 snmp_user_set                    MI  sup          0           0
L   2011 cli_config_io                    MI  gen        276           0
VRTR:
    2001 tmnxVRtrMidRouteTCA              MI  gen          0           0
    2002 tmnxVRtrHighRouteTCA             MI  gen          0           0
    2003 tmnxVRtrHighRouteCleared         MI  gen          0           0
    2004 tmnxVRtrIllegalLabelTCA          MA  gen          0           0
    2008 tmnxVRtrMaxArpEntriesTCA         MA  gen          0           0
    2009 tmnxVRtrMaxArpEntriesCleared     MI  gen          0           0
    2011 tmnxVRtrMaxRoutes                MI  gen          0           0
    2012 tmnxVRtrBfdSessionDown           MA  gen          0           0
    2013 tmnxVRtrBfdMaxSessionOnSlot      MA  gen          0           0
    2014 tmnxVRtrBfdPortTypeNotSupported  MA  gen          0           0
    2015 tmnxVRtrBfdSessionUp             MA  gen          0           0
    2016 tmnxVRtrIPv6MidRouteTCA          MI  gen          0           0
    2017 tmnxVRtrIPv6HighRouteTCA         MI  gen          0           0
    2018 tmnxVRtrIPv6HighRouteCleared     MI  gen          0           0
    2019 tmnxVRtrStaticRouteCPEStatus     MI  gen          0           0
    2020 tmnxVRtrBfdSessionDeleted        MI  gen          0           0
```

```
   2021 tmnxVRtrBfdSessionProtChange     MI  gen          0           0
   2022 tmnxVRtrManagedRouteAddFailed    MI  gen          0           0
   2023 tmnxVRtrFibOccupancyThreshold    MI  sup          0           0
   2024 tmnxVRtrInetAddressAttachFailed  MI  gen          0           0
   2029 tmnxVRtrIfLdpSyncTimerStart      WA  sup          0           0
   2030 tmnxVRtrIfLdpSyncTimerStop       WA  sup          0           0
===============================================================================

A:ALA-1# show log event-control ospf
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                      P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 ospfVirtIfStateChange            WA  gen          0           0
   2002 ospfNbrStateChange               WA  gen          1           0
   2003 ospfVirtNbrStateChange           WA  gen          0           0
   2004 ospfIfConfigError                WA  gen          0           0
   2005 ospfVirtIfConfigError            WA  gen          0           0
   2006 ospfIfAuthFailure                WA  gen          0           0
   2007 ospfVirtIfAuthFailure            WA  gen          0           0
   2008 ospfIfRxBadPacket                WA  gen          0           0
   2009 ospfVirtIfRxBadPacket            WA  gen          0           0
   2010 ospfTxRetransmit                 WA  sup          0           0
   2011 ospfVirtIfTxRetransmit           WA  sup          0           0
   2012 ospfOriginateLsa                 WA  sup          0         404
   2013 ospfMaxAgeLsa                    WA  gen          3           0
   2014 ospfLsdbOverflow                 WA  gen          0           0
   2015 ospfLsdbApproachingOverflow      WA  gen          0           0
   2016 ospfIfStateChange                WA  gen          2           0
   2017 ospfNssaTranslatorStatusChange   WA  gen          0           0
   2018 vRtrOspfSpfRunsStopped           WA  gen          0           0
   2019 vRtrOspfSpfRunsRestarted         WA  gen          0           0
   2020 vRtrOspfOverloadEntered          WA  gen          1           0
   2021 vRtrOspfOverloadExited           WA  gen          0           0
   2022 ospfRestartStatusChange          WA  gen          0           0
   2023 ospfNbrRestartHelperStatusChange WA  gen          0           0
   2024 ospfVirtNbrRestartHelperStsChg   WA  gen          0           0
===============================================================================
A:ALA-1#


A:ALA-1# show log event-control ospf ospfVirtIfStateChange
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                      P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 ospfVirtIfStateChange            WA  gen          0           0
===============================================================================
A:ALA-1#
```

Table 56: Output fields: event control

Label	Description
Application	Displays the application name
ID#	Displays the event ID number within the application L ID#

Label	Description
	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	Displays the event name
P	CL — The event has a cleared severity/priority CR — The event has critical severity/priority IN — The event has indeterminate severity/priority MA — The event has major severity/priority MI — The event has minor severity/priority WA — The event has warning severity/priority
g/s	gen — The event will be generated or logged by event control sup — The event will be suppressed or dropped by event control thr — Specifies that throttling is enabled
Logged	Displays the number of events logged or generated
Dropped	Displays the number of events dropped or suppressed

file-id

Syntax

file-id [*log-file-id*]

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

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 about the event file log.

Parameters

log-file-id

Displays detailed information about the specified event file log.

Values 1 to 99

Output

The following output is an example of event file information, and Table 57: Output fields: log file ID describes the output fields.

Sample output

```
*A:MTUSN945189# show log file-id
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
---------------------------------------------------------------
1         30       500        cf1:      none      cf1:
2         30       500        cf1:      none      cf1:
3         30       500        cf1:      none      cf1:
4         30       500        cf1:      none      cf1:
5         30       500        cf1:      none      cf1:
6         30       500        cf1:      none      cf1:
7         30       500        cf1:      none      cf1:
8         30       500        cf1:      none      cf1:
9         30       500        cf1:      none      cf1:
10        30       500        cf1:      none      cf1:
11        30       500        cf1:      none      cf1:
12        30       500        cf1:      none      cf1:
13        30       500        cf1:      none      cf1:
14        30       500        cf1:      none      cf1:
15        30       500        cf1:      none      cf1:
16        30       500        cf1:      none      cf1:
17        30       500        cf1:      none      cf1:
18        30       500        cf1:      none      cf1:
===============================================================
*A:MTUSN945189#

A:MTUSN945189# show log file-id 1
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
---------------------------------------------------------------
1         2800       500        cf1:      none      cf1:
===============================================================
===================================================================
File Id 1  Location cf1:
===================================================================
file name                                 expired   state
-------------------------------------------------------------------
cf1:\act\act0101-20010518-085306.xml.gz no        complete
===================================================================
*A:MTUSN945189#
```

Table 57: Output fields: log file ID

Label	Description
file-id	Displays the log file ID

Label	Description
rollover	Displays the rollover time for the log file which is how long in between partitioning of the file into a new file
retention	Displays 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	Displays the actual flash device on which the log file exists
file-id	Displays the log file ID
rollover	Displays the rollover time for the log file which is how long in between partitioning of the file into a new file
retention	Displays the retention time for the file in the system which is how long the file should be retained in the file system
file name	Displays 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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays event log filter policy information.

Parameters

filter-id

Displays detailed information about the specified event filter policy ID.

Values 1 to 65535

Output

The following outputs are examples of event log filter information, and the associated table describe the output fields.

- Sample output — summary, Table 58: Output fields: log filter summary
- Sample output — detailed, Table 59: Output fields: log filter detail

Sample output — summary

```
*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#
```

Table 58: Output fields: log filter summary

Label	Description
Filter Id	Displays 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	Displays the description string for the filter ID

Sample output — detailed

```
*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#
```

Table 59: Output fields: log filter detail

Label	Description
Filter-id	Displays 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)	Displays the description string for the filter ID
Entry-id	Displays the event log filter entry ID
Action	default — There is no explicit action for the event log filter entry and the filter 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)	Displays the description string for the event log filter entry
Application	Displays the event log filter entry application match criterion
Event Number	Displays 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

Label	Description
	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 GreaterThan — Matches when greater than the match criterion greaterThanOrEqual — Matches when greater than or equal to the match criterion lessThan — Matches when less than the match criterion lessThanOrEqual — Matches when less than or equal to the match criterion notEqual — Matches when not equal to the match criterion off — No operator specified for the match criterion

log-collector

Syntax

log-collector

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command displays log collector statistics for the main, security, change and debug log collectors.

Output

The following output is an example of log collector information, and Table 60: Output fields: log collector describes the output fields.

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#
```

Table 60: Output fields: log collector

Label	Description
<Collector Name>	Main The main event stream contains the events that are not explicitly directed to any other event stream.
	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

Label	Description
	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

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

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 to 99

severity-level

Displays only events with the specified and higher severity.

Default all severity levels

Values cleared, indeterminate, critical, major, minor, warning

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.

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 to 4294967295

count

Limits the number of log entries displayed to the number specified.

Default all log entries

Values 1 to 4294967295

router-instance

Specifies a router name up to 32 characters to be used in the display criteria.

subject

Displays only log entries matching the specified text *subject* string, up to 32 characters. 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 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

The following outputs are examples of event log summary information, and Table 61: Output fields: log ID describes the output fields.

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 output for memory or file event log contents

```
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: inSe
rvice"
....
===============================================================================
A:NS061550532>config>log>snmp-trap-group#
```

Table 61: Output fields: log ID

Label	Description
Log Id	Displays 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	Displays the index to the entry that defines the filter to be applied to this log source event stream to limit the events output to this log destination If the value is 0, 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	Displays the number of events that have been sent to the log sources that were forwarded to the log destination
Dropped	Displays the number of events sent to the log sources that were not forwarded to the log destination because they were filtered out by the log filter
Dest. Type	Console — All selected log events are directed to the system console If the console is not connected, all entries are dropped Syslog — All selected log events are sent to the syslog address

Label	Description
	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

snmp-trap-group

Syntax

snmp-trap-group [*log-id*]

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command displays SNMP trap group configuration information.

Parameters

log-id

Displays SNMP trap group information only for the specified trap group log ID.

Values 1 to 100

Output

The following output is an example of SNMP trap group information, and Table 62: Output fields: SNMP trap group describes the output fields.

Sample 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     : 10.20.20.5
Port        : 162
Version     : v2c
Community   : ntttesting
Sec. Level  : none
===============================================================================
A:SetupCLI>config>log>snmp-trap-group#
```

Table 62: Output fields: SNMP trap group

Label	Description
Log-ID	The log destination ID for an event stream.
Address	The IP address of the trap receiver,
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are 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.

syslog

Syntax

syslog [*syslog-id*]

Context

show>log

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command displays syslog event log destination summary information or detailed information about a specific syslog destination.

Parameters

syslog-id

Displays detailed information about the specified syslog event log destination.

Values 1 to 10

Output

The following output is an example of syslog information, and Table 63: Output fields: syslog describes the output fields.

Sample 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#
```

Table 63: Output fields: syslog

Label	Description
Syslog ID	Displays the syslog ID number for the syslog destination
IP Address	Displays the IP address of the syslog target host
Port	Displays the configured UDP port number used when sending syslog messages
Facility	Displays the facility code for messages sent to the syslog target host
Severity Level	Displays the syslog message severity level threshold
Below Level Dropped	Displays 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	Displays a text description stored in the configuration file for a configuration context
LogPrefix	Displays the prefix string prepended to the syslog message
Log-id	Events are directed to this *destination*

5.7.2.3 Clear commands

log

Syntax

log *log-id*

Context

clear

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

This command reinitializes the specified memory or 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 or session logs are not affected by this command.

Parameters

log-id

Specifies the event log ID to be initialized or rolled over.

Values 1 to 100

6 Facility alarms

This chapter provides information about configuring facility alarms.

6.1 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 alarm model is based on RFC 3877, *Alarm Management Information Base (MIB)*, (which evolved from the IETF DISMAN drafts).

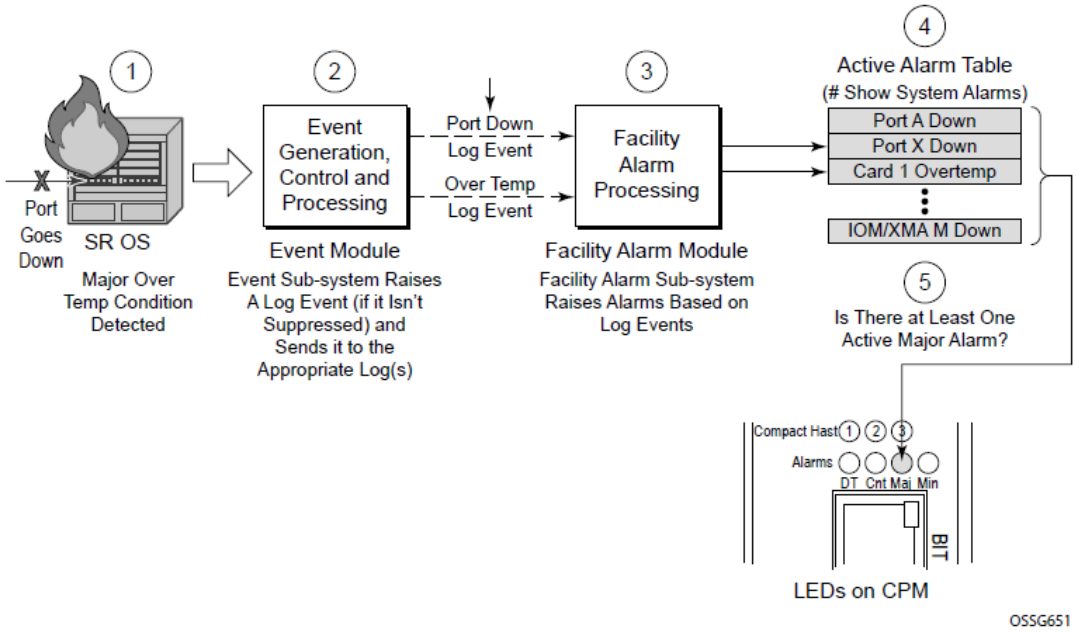
6.2 Facility alarms vs. log events

Facility Alarms are different from 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 modeled with state transition events (raised, cleared).

The Facility Alarms module processes log events 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.

The following figure shows the relationship of log events, alarms and the LEDs.

Figure 9: Log events, alarms and LEDs



Note:
On platforms that do not support Critical, Major, and Minor LED and Alarm output pins, an event is raised and only a log is generated.

Facility Alarms are different and have independent functionality from other uses of the term "alarm", such as:

- **configure port ethernet report-alarm**
- **configure system thresholds no memory-use-alarm**
- **configure system thresholds rmon no alarm**

6.3 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 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.

6.4 Facility alarm hierarchy

Facility Alarms for children objects is not raised for failure of a parent object. For example, when port fails (or is shut down) 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 shut down the port alarm is cleared (and a card alarm will be active). 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

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.

6.5 Facility alarm list

The following tables list the supported Facility Alarms.

Table 64: 7210 SAS supported facility alarms

Alarm	Alarm name/ raising event	Details string example	Clearing event	7210 SAS platforms					
				7210 SAS-T	7210 SAS-Mxp	7210 SAS-R6 and 7210 SAS-R12	7210 SAS-Sx 1/10GE	7210 SAS-S 1/10GE	7210 SAS-Sx 10/100GE
7-2001-1	tmnxEqCard Failure	Class MDA Module: failed, reason: MDA 1 failed startup tests	tmnxChassis NotificationClear			✓		✓	✓
7-2003-1	tmnxEqCard Removed	Class CPM Module: removed	tmnxEqCard Inserted			✓		✓	✓
7-2004-1	tmnxEqWrong Card	Class IOM Module: wrong type inserted	tmnxChassis NotificationClear			✓		✓	✓
7-2005-1	tmnxEnvTempToo High	Chassis 1: temperature too high	tmnxChassis NotificationClear	✓	✓	✓	✓	✓	✓
7-2006-1	tmnxEqFan Failure	Fan 1 failed	tmnxChassis NotificationClear	✓	✓	✓	✓	✓	✓
7-2007-1	tmnxEqPower SupplyFailureOvt	Power supply 2 over temperature	tmnxChassis NotificationClear						
7-2008-1	tmnxEqPower SupplyFailureAc	Power supply 1 AC failure	tmnxChassis NotificationClear						
7-2009-1	tmnxEqPower SupplyFailureDc	Power supply 2 DC failure	tmnxChassis NotificationClear						
7-2011-1	tmnxEqPower SupplyRemoved	Power supply 1, power lost	tmnxEqPower SupplyInserted	✓ [11]	✓ [11]	✓	✓ [11]	✓	✓
7-2017-1	tmnxEqSync IfTimingHoldover	Synchronous Timing interface in holdover state	tmnxEqSync IfTiming HoldoverClear	✓	✓	✓	✓	✓	✓

[11] ETR and non-ETR

Alarm	Alarm name/ raising event	Details string example	Clearing event	7210 SAS platforms					
				7210 SAS-T	7210 SAS-Mxp	7210 SAS-R6 and 7210 SAS-R12	7210 SAS-Sx 1/10GE	7210 SAS-S 1/10GE	7210 SAS-Sx 10/100GE
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Synchronous Timing interface, alarm los on reference 1	tmnxEqSyncIfTimingRef1AlarmClear	✓	✓	✓	✓	✓	✓
7-2019-2	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oof(2)'	Synchronous Timing interface, alarm of on reference 1	same as 7-2019-1	✓	✓	✓	✓	✓	✓
7-2019-3	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	Synchronous Timing interface, alarm oopir on reference 1	same as 7-2019-1	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓
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	✓	✓	✓		✓	✓
7-2033-1	tmnxChassisUpgradeInProgress	Class CPM Module: software upgrade in progress	tmnxChassisUpgradeComplete						
7-2050-1	tmnxEqPowerSupplyFailureInput	Power supply 1 input failure	tmnxChassisNotificationClear	✓	✓	✓	✓	✓	✓
7-2051-1	tmnxEqPowerSupplyFailureOutput	Power supply 1 output failure	tmnxChassisNotificationClear	✓	✓	✓	✓	✓	✓

Alarm	Alarm name/ raising event	Details string example	Clearing event	7210 SAS platforms					
				7210 SAS-T	7210 SAS-Mxp	7210 SAS-R6 and 7210 SAS-R12	7210 SAS-Sx 1/10GE	7210 SAS-S 1/10GE	7210 SAS-Sx 10/100GE
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	✓	✓				
3-2004-1	linkDown	Interface intf-towards-node-B22 is not operational	linkUp	✓	✓	✓	✓	✓	✓

The linkDown Facility Alarm is supported for the following objects:

Table 65: linkDown Facility Alarm support

Object	Alarm support
Ethernet Ports	Yes
Ethernet LAGs	No
Ethernet VLANs	No

6.6 Configuring logging with CLI

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

6.6.1 Basic facility alarm configuration

The most basic facility alarm configuration must have the following:

- log ID or accounting policy ID
- a log source
- a log destination

Example: Alarm configuration output

```
*7210SAS>config>system>alarms# info detail
----------------------------------------------
            no shutdown
            exit
----------------------------------------------
*7210SAS>config>system>alarms#
```

6.6.2 Common configuration tasks

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

6.6.2.1 Configuring the maximum number of alarms to clear

The number of alarms to clear can be configured using the command below.

Use the following syntax to configure a log file.

```
config>system
        alarms
            max-cleared max-alarms
```

Example: Facility alarm configuration output

```
ALA-12>config>system# alarms
------------------------------------------------
...
max-cleared 500
exit
...
------------------------------------------------
```

6.7 Facility alarms command reference

6.7.1 Command hierarchies

- Facility alarm configuration commands
- Show commands

6.7.1.1 Facility alarm configuration commands

```
config
    - system
        - alarms
            - max-cleared maximum
            - [no] shutdown
```

6.7.1.2 Show commands

```
show
    - system
        - alarms [cleared] [severity severity-level] [count count] [newer-than days]
```

6.7.2 Command descriptions

6.7.2.1 Configuration commands

alarms

Syntax

alarms

Context

config>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode.

Description

Commands in this context configure facility alarm parameters.

max-cleared

Syntax

max-cleared *maximum*

Context

config>system>alarms

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command configures the maximum number of cleared alarms that the system will store and display.

Default

500

Parameters

maximum

Specifies the maximum number of cleared alarms.

Values 0 to 500

shutdown

Syntax

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

Context

config>system>alarms

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

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 and CFMs. When facility alarm functionality is enabled, the alarms are viewed using the **show system alarms** commands.

Note:
Shutting down the system alarms clears all existing alarms (raised and cleared). Performing **no shutdown** will not bring back the earlier raised alarm.

Default

no shutdown

6.7.2.2 Show commands

alarms

Syntax

alarms [**cleared**] [**severity** *severity-level*] [**count** *count*] [**newer-than** *days*]

Context

show>system

Platforms

Supported on all 7210 SAS platforms as described in this document, including those configured in the access-uplink operating mode

Description

This command displays facility alarms on the system.

Parameters

cleared

Displays the cleared alarm queue.

severity-level

Specifies the severity level of the alarm.

Values critical | major | minor | warning

days

Displays alarms that are newer than the number of days specified.

Values 1 to 365

Output

The following output is an example of facility alarm information, and Table 66: Output fields: alarms describes the output fields.

Sample output

```
*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
===============================================================================
```

Table 66: Output fields: alarms

Label	Description
Index	Displays the alarm index number
Date/Time	Displays the date and time string for the alarm
Severity	Displays the severity level of the alarm
Alarm	Displays the alarm identifier
Resource	Displays the facility associated with the alarm
Details	Displays the description of the alarm

7 Appendix: accounting record name details for 7210 SAS platforms

This chapter provides information about accounting record name details for the 7210 SAS platforms.

7.1 Accounting record name details for 7210 SAS-T (access-uplink or network mode)

The following table lists the accounting policy record names and statistics on the 7210 SAS-T operating in access-uplink mode or network mode.

Table 67: Accounting record name details for 7210 SAS-T in access-uplink and network mode

Record name	Sub records	Sub record fields	Field description	Supported operating modes
Service-ingress-octets (counter mode is **in-out-profile-count**)	sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctets Forwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
Service-ingress-octets (counter mode is **forward-drop-count**)	sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		of	OctetsForwarded	
		od	OctetsDropped	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
Service-egress-octets **Note**: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	seo	(Per SAP)	(Per SAP)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
Service-ingress-packets (counter mode is **in-out-profile-count**)	sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		ipf	InProfilePktsForwarded	
		opf	OutOfProfilePktsForwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
Service-ingress-packets (counter mode is **forward-drop-count**)	sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		pf	PacketsForwarded	
		pd	PacketsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
Service-egress-packets. **Note**: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	sep	(Per SAP)	(Per SAP)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		pf	PktsForwarded	
		pd	PktsDropped	
Combined-service-ingress (counter mode is **in-out-profile-count**)	sio, sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctets Forwarded	
		ipf	InProfilePktsForwarded	
		opf	OutOfProfilePktsForwarded	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		ipo	IngressPktsOffered	
Combined-service-ingress (counter mode is **forward-drop-count**)	sio, sip	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		pf	PacketsForwarded	
		pd	PacketsDropped	
		of	OctetsForwarded	
		od	OctetsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
		ipo	IngressPktsOffered	
Combined-service-egress **Note**: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.	seo, sep	(Per SAP)	(Per SAP)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
		pf	PktsForwarded	
		pd	PktsDropped	
Complete-service-ingress-egress (counter mode is **in-out-profile-**	sio, sip	(Per Meter)	(Per Meter)	Access Uplink Network

Record name	Sub records	Sub record fields	Field description	Supported operating modes
count) **Note**: The Per SAP Egress Meter record has additional fields only when SAP aggregate meter is in use.		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutOfProfileOctets Forwarded	
		ipf	InProfilePktsForwarded	
		opf	OutOfProfilePktsForwarded	
	seo, sep	(Per Sap)	(Per Sap)	
		svc	SvcId	
		sap	SapId	
		ioo	IngressOctetsOffered	
		ipo	IngressPktsOffered	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
		pf	PktsForwarded	
		pd	PktsDropped	
Complete-service-ingress-egress (counter mode is **forward-drop-count**)	sip, sio	(Per Meter)	(Per Meter)	Access Uplink Network
		svc	SvcId	
		sap	SapId	
		mId	MeterId	
		pf	PacketsForwarded	
		pd	PacketsDropped	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		of	OctetsForwarded	
		od	OctetsDropped	
		(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		ipo	IngressPktsOffered	
		ioo	IngressOctetsOffered	
	seo, sep	(Per SAP)	(Per SAP)	
		svc	SvcId	
		sap	SapId	
		eof	EgressOctetsForwarded	
		epf	EgressPktsForwarded	
		(Per SAP Egress Meter)	(Per SAP Egress Meter)	
		mId	Egress Meter ID	
		of	OctetsForwarded	
		od	OctetsDropped	
		pf	PktsForwarded	
		pd	PktsDropped	
Access-egress-octets	aeo	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	Octets Dropped	
Access-egress-packets	aep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		pf	PktsForwarded	
		pd	PktsDropped	
Combined-access-egress	cmAeo , cm Aep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		pf	PktsForwarded	
		pd	PktsDropped	
		od	Octets Dropped	
Network-ingress-octets	nio	(Per Meter)	(Per Meter)	Access Uplink Network
		port	PortId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
Network-ingress-packets	nip	(Per Meter)	(Per Meter)	Access Uplink Network
		port	PortId	
		mId	MeterId	
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Network-egress-octets	neo	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	Octets Dropped	
Network-egress-packets	nep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		pf	PktsForwarded	
		pd	PktsDropped	
Combined-network-egress	cmNeo , cmNep	(Per Queue)	(Per Queue)	Access Uplink Network
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		pf	PktsForwarded	
		pd	PktsDropped	
		od	OctetsDropped	
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)	Access Uplink Network
		port	PortId	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
		(Per Queue)	(Per Queue)	
		port	PortId	
		qId	QueueId	
		of	OctetsForwarded	
		od	OctetsDropped	
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)	Network
		NwIf	IpInterface	
		mId	MeterId	
		iof	InProfileOctetsForwarded	
		oof	OutProfileOctetsForwarded	
		ipf	InProfilePktsForwarded	
		opf	OutProfilePktsForwarded	
Combined-sdp-ingress-egress	cm Sdpipo,cm Sdpepo cmSdpipo (Ingress)			Network
		svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
Complete-sdp-ingress-egress	cm Sdpipo,cm Sdpepo,cp Sdpipo,cp Sdpepo			Network
	cmSdpipo (Ingress)	svc	SvcID	
		sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cmSdpepo (Egress)	svc	SvcID	
		sdp	SdpID	

Record name	Sub records	Sub record fields	Field description	Supported operating modes
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cpSdpipo (Ingress)	sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	
	cpSdpepo (Egress)	sdp	SdpID	
		tpf	TotalPacketsForwarded	
		tof	TotalOctetsForwarded	

7.2 Accounting record name details for 7210 SAS-R6 and 7210 SAS-R12

The following table lists the accounting policy record names and statistics on the 7210 SAS-R6 and 7210 SAS-R12.

Table 68: Accounting record name details for 7210 SAS-R6 and 7210 SAS-R12

Record name	Sub records	Sub record fields	Field description
Access-ingress-octets (counter mode is **forward-drop-count**)	aio	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
Access-ingress-packet (counter mode is **forward-drop-count**)	aip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
Access-ingress-octets (counter mode is **in-out-profile-count**)	aio	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId

Record name	Sub records	Sub record fields	Field description
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Access-ingress-packets (counter mode is **in-out-profile-count**)	aip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Combined-access-ingress (counter mode is **forward-drop-count**)	cmAio, cmAip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Combined-access-ingress (counter mode is **in-out-profile-count**)	cmAio, cmAip	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Complete-access-ingress-egress (counter mode is **forward-drop-count**)	cpAio, cpAip, cpAeo, cpAep	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped

Record name	Sub records	Sub record fields	Field description
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Complete-access-ingress-egress (counter mode is **in-out-profile-count**)	cpAio, cpAip, cpAeo, cpAep	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Service-ingress-octets (counter mode is **in-out-profile-count**)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)

Record name	Sub records	Sub record fields	Field description
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-ingress-octets (counter mode is **forward-drop-count**)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		of	OctetsForwarded
		od	OctetsDropped

Record name	Sub records	Sub record fields	Field description
Service-ingress-packets (counter mode is **in-out-profile-count**)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPacketsOffered
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	IngressPacketsOffered
Service-egress-packets **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not	sep	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId

Record name	Sub records	Sub record fields	Field description
available in SAP based queuing and scheduling mode.		sap	SapId
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		pf	PacketsForwarded
		pd	PacketsDropped
Combined-service-ingress (counter mode is **in-out-profile-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-ingress (counter mode is **forward-drop-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)

Record name	Sub records	Sub record fields	Field description
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-egress **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Complete-service-ingress-egress (counter mode is **in-out-profile-count**) **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based	sio, sip	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded

Record name	Sub records	Sub record fields	Field description
queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
	seo, sep	(Per Sap)	(Per Sap)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped

Record name	Sub records	Sub record fields	Field description
Complete-service-ingress-egress (counter mode is **forward-drop-count**) **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used. In addition, the SAP egress meter counters is available only with port-based queuing and scheduling and when SAP aggregate meter has been enabled for the SAP. It is not available in SAP based queuing and scheduling mode.	sip, sio	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
		(Per SAP Egress Meter)	(Per SAP Egress Meter)
		mId	Egress Meter ID

Record name	Sub records	Sub record fields	Field description
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Access-egress-octets **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	aeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Access-egress-packets **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	aep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-access-egress **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	cmAeo , cm Aep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
		od	Octets Dropped
Network-ingress-octets	nio	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-ingress-packets	nip	(Per Meter)	(Per Meter)
		port	PortId

Record name	Sub records	Sub record fields	Field description
		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 , cm Nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
		od	OctetsDropped
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId

Record name	Sub records	Sub record fields	Field description
		of	OctetsForwarded
		od	OctetsDropped
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-sdp-ingress-egress	cmSdpipo,cmSdpepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

Record name	Sub records	Sub record fields	Field description
Complete-sdp-ingress-egress	cmSdpipo,cmSdpepo,cpSdpipo,cpSdpepo		
	cmSdpipo (Ingress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo (Ingress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo (Egress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

7.3 Accounting record name details for 7210 SAS-Mxp

The following table lists the accounting policy record names and statistics for 7210 SAS-Mxp.

Table 69: Accounting record name details for 7210 SAS-Mxp

Record name	Sub records	Sub record fields	Field description
Access-ingress-octets (counter mode is **forward-drop-count**)	aio	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped

Record name	Sub records	Sub record fields	Field description
Access-ingress-packet (counter mode is **forward-drop-count**)	aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
Access-ingress-octets (counter mode is **in-out-profile-count**)	aio	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Access-ingress-packets (counter mode is **in-out-profile-count**)	aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Combined-access-ingress (counter mode is **forward-drop-count**)	aio, aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Combined-access-ingress (counter mode is **in-out-profile-count**)	aio, aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded

Record name	Sub records	Sub record fields	Field description
		opf	OutProfilePacketsForwarded
Complete-access-ingress-egress (counter mode is **forward-drop-count**)	aio, aip, aeo, aep	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Complete-access-ingress-egress (counter mode is **in-out-profile-count**)	aio, aip, aeo, aep	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded

Record name	Sub records	Sub record fields	Field description
		opf	OutProfilePacketsForwarded
Service-ingress-octets (counter mode is **in-out-profile-count**)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-ingress-octets (counter mode is **forward-drop-count**)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-egress-octets **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	seo	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)

Record name	Sub records	Sub record fields	Field description
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
Service-ingress-packets (counter mode is **in-out-profile-count**)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ipo	IngressPacketsOffered
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	IngressPacketsOffered
Service-egress-packets **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sep	(Per Egress queue)	(Per Egress queue)
		svc	SvcId
		sap	SapId
		qid	Egress QueueId
		pf	PacketsForwarded

Record name	Sub records	Sub record fields	Field description
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPktsForwarded
Combined-service-ingress (counter mode is **in-out-profile-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-ingress (counter mode is **forward-drop-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId

Record name	Sub records	Sub record fields	Field description
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
Combined-service-egress **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Complete-service-ingress-egress (counter mode is **in-out-profile-count**) **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sio, sip	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
	seo, sep	(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered

Record name	Sub records	Sub record fields	Field description
		ipo	IngressPktsOffered
	seo, sep	(Per Egress Queue)	(Per Egress Queue)
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPacketsForwarded
Complete-service-ingress-egress (counter mode is **forward-drop-count**) **Note**: The Per SAP egress queue counters are available only when SAP based queuing and scheduling is used. It is not available when port-based queuing and scheduling is used.	sip, sio	(Per Ingress Meter)	(Per Ingress Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPacketsOffered
	seo, sep	(Per Egress Queue)	(Per Egress Queue)

Record name	Sub records	Sub record fields	Field description
		svc	SvcId
		sap	SapId
		qid	EgressQueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Access-egress-octets **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	aeo	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	Octets Dropped
Access-egress-packets **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	aep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		pf	PktsForwarded
		pd	PktsDropped
Combined-access-egress **Note:** This accounting record is applicable only when port-based queuing and scheduling is used. It it not available in SAP based queuing and scheduling.	cmAeo , cm Aep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped

Record name	Sub records	Sub record fields	Field description
		od	Octets Dropped
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 , cm Nep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
		od	OctetsDropped

Record name	Sub records	Sub record fields	Field description
Combined-network-ing-egr-octets	cmNio,cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-sdp-ingress-egress			

Record name	Sub records	Sub record fields	Field description
	cmSdpipo,cmSdpepo cmSdpipo (Ingress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
Complete-sdp-ingress-egress	cmSdpipo,cmSdpepo,cpSdpipo,cpSdpepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo (Ingress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo (Egress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

7.4 Accounting record name details for 7210 SAS-Sx/S 1/10GE and 7210 SAS-Sx 10/100GE

The following table lists the accounting policy record names and the statistics for the 7210 SAS-Sx/S 1/10GE and 7210 SAS-Sx 10/100GE.

Table 70: Accounting record name details for 7210 SAS-Sx/S 1/10GE and 7210 SAS-Sx 10/100GE

Record name	Sub records	Sub record fields	Field description
Access-ingress-octets (counter mode is **forward-drop-count**)	aio	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
Access-ingress-packet (counter mode is **forward-drop-count**)	aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		pf	PacketsForwarded
		pd	PacketsDropped
Access-ingress-octets (counter mode is **in-out-profile-count**)	aio	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Access-ingress-packets (counter mode is **in-out-profile-count**)	aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Combined-access-ingress (counter mode is **forward-drop-count**)	aio, aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded

Record name	Sub records	Sub record fields	Field description
		pd	PacketsDropped
Combined-access-ingress (counter mode is **in-out-profile-count**)	aio, aip	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Complete-access-ingress-egress (counter mode is **forward-drop-count**)	aio, aip, aeo, aep	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
		pf	PacketsForwarded
		pd	PacketsDropped
Complete-access-ingress-egress (counter mode is **in-out-profile-count**)	aio, aip, aeo, aep	(Per Meter)	(Per Meter)
		pId	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded

Record name	Sub records	Sub record fields	Field description
		opf	OutProfilePacketsForwarded
		(Per Queue)	(Per Queue)
		pId	PortId
		mId	QueueId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePacketsForwarded
		opf	OutProfilePacketsForwarded
Service-ingress-octets (counter mode is **in-out-profile-coun**t)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
Service-ingress-octets (counter mode is **forward-drop-count**)	sio	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		of	OctetsForwarded
		od	OctetsDropped
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered

Record name	Sub records	Sub record fields	Field description
Service-egress-octets	seo	(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
Service-ingress-packets (counter mode is **in-out-profile-count**)	sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(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
Service-egress-packets	sep	(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		epf	EgressPktsForwarded

Record name	Sub records	Sub record fields	Field description
Combined-service-ingress (counter mode is **in-out-profile-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
Combined-service-ingress (counter mode is **forward-drop-count**)	sio, sip	(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
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
Combined-service-egress	seo, sep	(Per SAP)	(Per SAP)
		svc	SvcId

Record name	Sub records	Sub record fields	Field description
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Complete-service-ingress-egress (counter mode is **in-out-profile-count**)	sio, sip	(Per Meter)	(Per Meter)
		svc	SvcId
		sap	SapId
	seo, sep	mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		ioo	IngressOctetsOffered
		ipo	IngressPktsOffered
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Complete-service-ingress-egress (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

Record name	Sub records	Sub record fields	Field description
		sap	SapId
		ipo	IngressPktsOffered
		ioo	IngressOctetsOffered
	seo, sep	(Per SAP)	(Per SAP)
		svc	SvcId
		sap	SapId
		eof	EgressOctetsForwarded
		epf	EgressPktsForwarded
Access-egress-octets	aeo	(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
Combined-access-egress	cmAeo , cmAep	(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		pf	PktsForwarded
		pd	PktsDropped
		od	Octets Dropped
Network-ingress-octets	nio	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId

Record name	Sub records	Sub record fields	Field description
		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	OctetsDropped
Combined-network-ing-egr-octets	cmNio, cmNeo	(Per Meter)	(Per Meter)
		port	PortId
		mId	MeterId
		iof	InProfileOctetsForwarded

Record name	Sub records	Sub record fields	Field description
		oof	OutProfileOctetsForwarded
		(Per Queue)	(Per Queue)
		port	PortId
		qId	QueueId
		of	OctetsForwarded
		od	OctetsDropped
Network-interface-ingress-octets	niio	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
Network-interface-ingress-packets	niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-network-interface-ingress	niio , niip	(Per Meter)	(Per Meter)
		NwIf	IpInterface
		mId	MeterId
		iof	InProfileOctetsForwarded
		oof	OutProfileOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutProfilePktsForwarded
Combined-sdp-ingress-egress	cmSdpipo,cmSdpepo cmSdpipo (Ingress)		
		svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

Record name	Sub records	Sub record fields	Field description
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
Complete-sdp-ingress-egress	cmSdpipo,cmSdpepo,cpSdpipo,cpSdpepo		
	cmSdpipo (Ingress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cmSdpepo (Egress)	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo (Ingress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpepo (Egress)	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

8 Standards and protocol support

Note:
The information provided in this chapter is subject to change without notice and may not apply to all platforms.

Nokia assumes no responsibility for inaccuracies.

The following conventions are used in this section:

- T(A,N) means 7210 SAS-T in both Access-uplink mode and Network mode. Similarly T(N) means 7210 SAS-T in network mode only.
- K5 indicates 7210 SAS-K 2F2T1C.
- K12 indicates 7210 SAS-K 2F4T6C.
- K30 indicates 7210 SAS-K 3SFP+ 8C.
- Sx/S-1/10GE indicates all variants of 7210 SAS-Sx 1/10GE and 7210 SAS-S 1/10GE platforms.
- Sx-10/100GE indicates only the variants of 7210 SAS-Sx 10/100GE. Sx-10/100GE QSFP28 indicates the 7210 SAS-Sx 10/100GE 64 SFP+ 4QSFP28 variant.
- Sx/S-1/10GE-VC indicates 7210 SAS-Sx 1/10GE and 7210 SAS-S 1/10GE platforms in standalone VC mode.
- R6 indicates 7210 SAS-R6.
- R12 indicates 7210 SAS-R12.
- D indicates 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.
- Dxp indicates 7210 SAS-Dxp-12p (2SFP+ 4F6T), 7210 SAS-Dxp-12p ETR (2SFP+ 4F6T), 7210 SAS-Dxp 16p (2SFP+ 4F10T), and 7210 SAS-Dxp-24p (2SFP+ 6F16T). If a line item applies only to a particular variant, the variant name will be called out explicitly against that item.
- This standards list is not applicable to platforms in the satellite mode of operation, as most of the features are supported on 7x50 SR platforms. For this reason, the host platforms standards compliancemust be consulted for the satellite mode of operation.

8.1 BGP

draft-ietf-idr-add-paths-04, Advertisement of Multiple Paths in BGP is supported on T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-sidr-origin-validation-signaling-04, BGP Prefix Origin Validation State Extended Community is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1772, Application of the Border Gateway Protocol in the Internet is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1997, BGP Communities Attribute is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2439, BGP Route Flap Damping is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2858, Multiprotocol Extensions for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2918, Route Refresh Capability for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3107, Carrying Label Information in BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3392, Capabilities Advertisement with BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4271, A Border Gateway Protocol 4 (BGP-4) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4360, BGP Extended Communities Attribute is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only R6 and R12 supports RR server functionality. Rest of the platforms support only client function.

RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4684, Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4724, Graceful Restart Mechanism for BGP (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4760, Multiprotocol Extensions for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4893, BGP Support for Four-octet AS Number Space is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5004, Avoid BGP Best Path Transitions from One External to Another is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5291, Outbound Route Filtering Capability for BGP-4 is supported on K12, K30, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5668, 4-Octet AS Specific BGP Extended Community is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6811, Prefix Origin Validation is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.2 Ethernet

IEEE 802.1AB, Station and Media Access Control Connectivity Discovery is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

TIA-1057, LLDP for Media endpoint devices is supported on Dxp, Sx/S-1/10GE, and Sx/S-1/10GE-VC

IEEE 802.1ad, Provider Bridges is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1ag, Connectivity Fault Management is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1ah, Provider Backbone Bridges is supported on T(N)

IEEE 802.1ax, Link Aggregation is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1D, MAC Bridges is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1p, Traffic Class Expediting is supported on D, E, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1Q, Virtual LANs is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1s, Multiple Spanning Trees is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1w, Rapid Reconfiguration of Spanning Tree is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1X, Port Based Network Access Control is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ab, 1000BASE-T is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ac, VLAN Tag is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ad, Link Aggregation is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ae, 10 Gb/s Ethernet is supported on Dxp, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ah, Ethernet in the First Mile is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ba, 40 Gb/s and 100 Gb/s Ethernet is supported on R6, R12, and Sx-10/100GE

IEEE 802.3i, Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3u, Fast Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3z, Gigabit Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3af, Power Over Ethernet (PoE) is supported on Dxp, T-ETR, Mxp-ETR, and Sx/S-1/10GE

Note:
Sx/S-1/10GE only on PoE variant and Sx-1/10GE fiber variant with two fixed copper ports). Only on Dxp-16p and Dxp-24p.

IEEE 802.3at, Power Over Ethernet (PoE+) is supported on Dxp, T-ETR, Mxp-ETR, and Sx/S-1/10GE

Note:
Sx/S-1/10GE only on PoE variant and Sx-1/10GE fiber variant with two fixed copper ports). Only on Dxp-16p and Dxp-24p.

IEEE 802.3bt, Power Over Ethernet (PoE++/HPoE) is supported on Dxp

Note:
Only on Dxp-16p and Dxp-24p.

ITU-T G.8032, Ethernet Ring Protection Switching is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.3 EVPN

draft-snr-bess-evpn-proxy-arp-nd-00, Proxy-ARP/ND function in EVPN networks is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

Note:
Sx/S-/10GE standalone mode only.

RFC 7432, BGP MPLS-Based Ethernet VPN is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

Note:
Sx/S-/10GE standalone mode only.

8.4 Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, Operational management of Loop Free Alternates is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7490, Remote Loop-Free Alternate (LFA) Fast Reroute (FRR) is supported on K12, K30, Mxp, Sx/S-1/10GE,R6, and R12

Note:
With Segment Routing.

8.5 Internet Protocol (IP) — General

draft-grant-tacacs-02, The TACACS+ Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-vrrp-unified-spec-02, Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6 is supported on Mxp

RFC 768, User Datagram Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 793, Transmission Control Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 854, TELNET Protocol Specifications is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 951, Bootstrap Protocol (BOOTP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1034, Domain Names - Concepts and Facilities is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1035, Domain Names - Implementation and Specification is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1350, The TFTP Protocol (revision 2) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1534, Interoperation between DHCP and BOOTP is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1542, Clarifications and Extensions for the Bootstrap Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2131, Dynamic Host Configuration Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2347, TFTP Option Extension is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2348, TFTP Blocksize Option is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2349, TFTP Timeout Interval and Transfer Size Options is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2428, FTP Extensions for IPv6 and NATs is supported on D, Dxp, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2865, Remote Authentication Dial In User Service (RADIUS) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2866, RADIUS Accounting is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3046, DHCP Relay Agent Information Option (Option 82) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3596, DNS Extensions to Support IP version 6 is supported on D, Dxp, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3768, Virtual Router Redundancy Protocol (VRRP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4251, The Secure Shell (SSH) Protocol Architecture is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4252, The Secure Shell (SSH) Authentication Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
All 7210 platforms support password and publickey based user authentication. 7210 SAS-D support only password based authentication.

RFC 4253, The Secure Shell (SSH) Transport Layer Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4254, The Secure Shell (SSH) Connection Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5880, Bidirectional Forwarding Detection (BFD) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 5881, Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 5883, Bidirectional Forwarding Detection (BFD) for Multihop Paths is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 6528, Defending against Sequence Number Attacks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7130, Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces is supported on T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

8.6 IP — Multicast

RFC 1112, Host Extensions for IP Multicasting is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IGMP v1, v2, v3 is supported.

RFC 2236, Internet Group Management Protocol, Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3376, Internet Group Management Protocol, Version 3 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3446, Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
MSDP supported only on Sx/S-1/10GE standalone.

RFC 3618, Multicast Source Discovery Protocol (MSDP) is supported on Sx/S-1/10GE

Note:
Only in standalone mode.

RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4604, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
MLD not supported.

RFC 4607, Source-Specific Multicast for IP is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4608, Source-Specific Protocol Independent Multicast in 232/8 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5059, Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5384, The Protocol Independent Multicast (PIM) Join Attribute Format is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6513, Multicast in MPLS/BGP IP VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6514, BGP Encodings and Procedures for Multicast in MPLS/IP VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6515, IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6625, Wildcards in Multicast VPN Auto-Discover Routes is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6826, Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 7246, Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 7385, IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

8.7 IP — Version 4

RFC 791, Internet Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 792, Internet Control Message Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 826, An Ethernet Address Resolution Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1812, Requirements for IPv4 Routers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1981, Path MTU Discovery for IP version 6 is supported on K12, K30, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2401, Security Architecture for Internet Protocol is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Supported only for OSPFv3 authentication. Not supported for services.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

8.8 IP — Version 6

RFC 2464, Transmission of IPv6 Packets over Ethernet Networks is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 3021, Using 31-Bit Prefixes on IPv4 Point-to-Point Links is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification is supported on K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3587, IPv6 Global Unicast Address Format is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4007, IPv6 Scoped Address Architecture is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4193, Unique Local IPv6 Unicast Addresses is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4291, Internet Protocol Version 6 (IPv6) Addressing Architecture is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4861, Neighbor Discovery for IP version 6 (IPv6) is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4862, IPv6 Stateless Address Autoconfiguration (Router Only) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5095, Deprecation of Type 0 Routing Headers in IPv6 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5952, A Recommendation for IPv6 Address Text Representation is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 6106, IPv6 Router Advertisement Options for DNS Configuration is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6164, Using 127-Bit IPv6 Prefixes on Inter-Router Links is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.9 IPsec

RFC 2401, Security Architecture for the Internet Protocol is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only for use with OSPFv3 authentication. Not supported for services.

RFC 2406, IP Encapsulating Security Payload (ESP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only for use with OSPFv3 authentication. Not supported for services.

8.10 IS-IS

draft-ietf-isis-mi-02, IS-IS Multi-Instance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-segment-routing-extensions-04, IS-IS Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

draft-kaplan-isis-ext-eth-02, Extended Ethernet Frame Size Support is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and 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) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3359, Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3719, Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3787, Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4971, Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5120, M-ISIS: Multi Topology (MT) Routing in IS-IS is supported on K12, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5301, Dynamic Hostname Exchange Mechanism for IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5302, Domain-wide Prefix Distribution with Two-Level IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5303, Three-Way Handshake for IS-IS Point-to-Point Adjacencies is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5304, IS-IS Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5305, IS-IS Extensions for Traffic Engineering TE is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5306, Restart Signaling for IS-IS (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5308, Routing IPv6 with IS-IS is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5310, IS-IS Generic Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6232, Purge Originator Identification TLV for IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6233, IS-IS Registry Extension for Purges is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-mi-02, IS-IS Multi-Instance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
K12, K30 support only a single instance and can operate in multi-instance deployment as it supports the processing of TLVs for multi-instance support.

draft-ietf-isis-segment-routing-extensions-04, IS-IS Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

8.11 Management

draft-ieft-snmpv3-update-mib-05, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-idr-bgp4-mib-05, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-wg-mib-06, Management Information Base for Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mboned-msdp-mib-01, Multicast Source Discovery protocol MIB is supported on Sx/S-1/10GE

Note:
Only in standalone mode.

draft-ietf-mpls-ldp-mib-07, Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mpls-lsr-mib-06, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mpls-te-mib-04, Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-mib-update-08, OSPF Version 2 Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaaddressfamilynumbers-mib, IANA-ADDRESS-FAMILY-NUMBERS-MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaiftype-mib, IANAifType-MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaiprouteprotocol-mib, IANA-RTPROTO-MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8021-CFM-MIB, IEEE P802.1ag(TM) CFM MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8021-PAE-MIB, IEEE 802.1X MIB is supported on D, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8023-LAG-MIB, IEEE 802.3ad MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

LLDP-MIB, IEEE P802.1AB(TM) LLDP MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1157, A Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1215, A Convention for Defining Traps for use with the SNMP is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1724, RIP Version 2 MIB Extension is supported on Mxp

RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2138, Remote Authentication Dial In User Service (RADIUS) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2206, RSVP Management Information Base using SMIv2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2213, Integrated Services Management Information Base using SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2571, An Architecture for Describing SNMP Management Frameworks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2573, SNMP Applications is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) is supported on D, E, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2578, Structure of Management Information Version 2 (SMIv2) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2579, Textual Conventions for SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2819, Remote Network Monitoring Management Information Base is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2856, Textual Conventions for Additional High Capacity Data Types is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2863, The Interfaces Group MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2864, The Inverted Stack Table Extension to the Interfaces Group MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2933, Internet Group Management Protocol MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3014, Notification Log MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3164, The BSD syslog Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3165, Definitions of Managed Objects for the Delegation of Management Scripts is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3231, Definitions of Managed Objects for Scheduling Management Operations is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3273, Remote Network Monitoring Management Information Base for High Capacity Networks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3419, Textual Conventions for Transport Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3593, Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals is supported on Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3635, Definitions of Managed Objects for the Ethernet-like Interface Types is supported on D, E, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3877, Alarm Management Information Base (MIB) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4001, Textual Conventions for Internet Network Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4022, Management Information Base for the Transmission Control Protocol (TCP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4113, Management Information Base for the User Datagram Protocol (UDP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4220, Traffic Engineering Link Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4292, IP Forwarding Table MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4293, Management Information Base for the Internet Protocol (IP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5101, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information is supported on Mxp, Sx/S-1/10GE, and R6

RFC 6241, Network Configuration Protocol (NETCONF) is supported on K5, K12, T(N), Mxp, Sx/S-1/10GE, R6, and R12

RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH) is supported on K5, K12, T(N), Mxp, Sx/S-1/10GE, R6, and R12

8.12 MPLS — General

RFC 3031, Multiprotocol Label Switching Architecture is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3032, MPLS Label Stack Encoding is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3443, Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4182, Removing a Restriction on the use of MPLS Explicit NULL is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5332, MPLS Multicast Encapsulations is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

8.13 MPLS — GMPLS

draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.14 MPLS — LDP

draft-ietf-mpls-ldp-ipv6-15, Updates to LDP for IPv6 is supported on Mxp

draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-pdutta-mpls-ldp-v2-00, LDP Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3037, LDP Applicability is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5036, LDP Specification is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5443, LDP IGP Synchronization is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5561, LDP Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
P2MP LSPs only.

8.15 MPLS — MPLS-TP

RFC 5586, MPLS Generic Associated Channel is supported on T(N), R6, and R12

RFC 5921, A Framework for MPLS in Transport Networks is supported on T(N), R6, and R12

RFC 5960, MPLS Transport Profile Data Plane Architecture is supported on T(N), R6, and R12

RFC 6370, MPLS Transport Profile (MPLS-TP) Identifiers is supported on T(N), R6, and R12

RFC 6378, MPLS Transport Profile (MPLS-TP) Linear Protection is supported on T(N), R6, and R12

RFC 6426, MPLS On-Demand Connectivity and Route Tracing is supported on T(N), R6, and R12

RFC 6428, Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile is supported on T(N), R6, and R12

RFC 6478, Pseudowire Status for Static Pseudowires is supported on T(N), R6, and R12

RFC 7213, MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing is supported on T(N), R6, and R12

8.16 MPLS — OAM

RFC 6424, Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6425, Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping is supported on T(N), Mxp, R6, and R12

8.17 MPLS — RSVP-TE

RFC 2702, Requirements for Traffic Engineering over MPLS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2747, RSVP Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2961, RSVP Refresh Overhead Reduction Extensions is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3097, RSVP Cryptographic Authentication -- Updated Message Type Value is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4561, Definition of a Record Route Object (RRO) Node-Id Sub-Object is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4875, Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4950, ICMP Extensions for Multiprotocol Label Switching is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5817, Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.18 OSPF

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

RFC 1765, OSPF Database Overflow is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2328, OSPF Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3509, Alternative Implementations of OSPF Area Border Routers is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3623, Graceful OSPF Restart Graceful OSPF Restart (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4222, Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4552, Authentication/Confidentiality for OSPFv3 is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4970, Extensions to OSPF for Advertising Optional Router Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5185, OSPF Multi-Area Adjacency is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5187, OSPFv3 Graceful Restart (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5243, OSPF Database Exchange Summary List Optimization is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5250, The OSPF Opaque LSA Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5340, OSPF for IPv6 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5838, Support of Address Families in OSPFv3 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6987, OSPF Stub Router Advertisement is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

8.19 Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, OAM Procedures for VPWS Interworking is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3916, Requirements for Pseudo- Wire Emulation Edge-to-Edge (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4385, Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4446, IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5659, An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6073, Segmented Pseudowire is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6310, Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network is supported on K12, K30, Mxp, R6, and R12

RFC 6718, Pseudowire Redundancy is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6870, Pseudowire Preferential Forwarding Status bit is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7023, MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7267, Dynamic Placement of Multi-Segment Pseudowires is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.20 Quality of Service

RFC 2430, A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2598, An Expedited Forwarding PHB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3140, Per Hop Behavior Identification Codes is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3260, New Terminology and Clarifications for Diffserv is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.21 RIP

RFC 1058, Routing Information Protocol is supported on Mxp

RFC 2082, RIP-2 MD5 Authentication is supported on Mxp

RFC 2453, RIP Version 2 is supported on Mxp

8.22 Timing

GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR. Dxp-ETR and Sx-10/100GE does not support IEEE default profile.

ITU-T G.781, Synchronization layer functions, issued 09/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8261, Timing and synchronization aspects in packet networks, issued 04/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8262, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8264, Distribution of timing information through packet networks, issued 10/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8265.1, Precision time protocol telecom profile for frequency synchronization, issued 10/2010 is supported on D-ETR, K5, K12, K30, T(A,N), Mxp, Sx-1/10GE, R6, and 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 is supported on Dxp, K12, K30, T(A,N), Mxp, Sx-1/10GE, Sx-10/100GE, R6, and R12

Note:
Only on 7210 SAS-Sx 10/100GE QSFP28 variant and Dxp-12p ETR.

IEC/IEEE 61850-9-3-2016, Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation is supported on Dxp-16p and Dxp-24p

IEEE C37.238-2017 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications is supported on Dxp-16p and Dxp-24p

RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

8.23 VPLS

RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

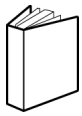
Note:
On 7210 platforms, only BGP-AD is suported with TLDP signalling for PW. No BGP signalling is supported for PW establishment.

RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5501, Requirements for Multicast Support in Virtual Private LAN Services is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback