7705 Service Aggregation Router

Release 24.10.R1

System Management Guide

3HE 20402 AAAB TQZZA
Edition: 01
October 2024

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 Preface

This guide describes router security, SNMP features, and event and accounting logs. It covers basic tasks such as configuring management access filters that control traffic in and out of the CSM, passwords, user profiles, and security such as RADIUS, TACACS+, and SSH servers.

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

Note: This manual generically covers Release 24.x content and may contain some content that will be released in later maintenance loads. Please see the 7705 SAR 24.x.Rx Software Release Notes, part number 3HE20411000xTQZZA, for information about features supported in each load of the Release 24.x software.

Note: As of Release 23.4, software support for the following hardware has been deprecated:

- 8-port Ethernet Adapter card, version 2 (a8-ethv2) (3HE02776)
- 12-port Serial Data Interface card, version 1 (a12-sdi) (3HE03391)
- 7705 SAR-W (3HE07349)

These components are no longer recognized in the release.

If information about any of the above components is required, please see the applicable installation guides in Release 22.10.

1.1 Audience

This guide is intended for network administrators who are responsible for configuring the 7705 SAR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Concepts described in this guide include the following:

- CLI concepts
- system and user access and security
- SNMP
- event and accounting logs

1.2 Technical support

If you purchased a service agreement for your 7705 SAR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased a Nokia service agreement, follow this link to contact a Nokia support representative and to access product manuals and documentation updates:

Product Support Portal

2 7705 SAR system management configuration process

The following table lists the tasks that are required to configure system security and access functions as well as event and accounting logs.

Each chapter in this book is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration process

Area	Task/description	Chapter
System security	Configure system security parameters, such as authentication, authorization, and accounting	Security
Network management	Configure SNMP elements	SNMP
Operational functions	Configure event and accounting logs	Event and accounting logs
Reference	List of security and telecom standards, supported protocols, and proprietary MIBs	Supported standards and protocols

3 Security

This chapter provides information to configure security parameters.

Topics in this chapter include:

3.1 Authentication, authorization, and accounting

This section describes authentication, authorization, and accounting (AAA) used to monitor and control network access on the 7705 SAR. Network security is based on a multi-step process. The first step, authentication, validates a user's name and password. The second step is authorization, which allows the user to access and execute commands at various command levels based on profiles assigned to the user.

The third 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.

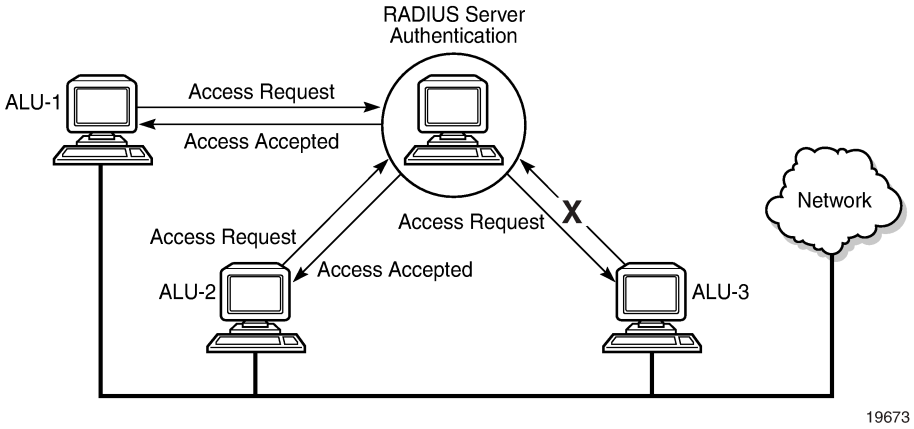
You can configure the 7705 SAR to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, SSH, SFTP, SCP, or FTP. You can select the authentication order that determines the authentication method to try first, second, and third.

The 7705 SAR 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 depicts end-user access requests sent to a RADIUS server. After validating the usernames and passwords, the RADIUS server returns an access accept message to the users on ALU-1 and ALU-2. The username and password from ALU-3 could not be authenticated; therefore, access was denied.

Figure 1: RADIUS requests and responses



3.1.1 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 or through Telnet, SSH, SFTP, SCP, or FTP, the 7705 SAR 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. Up to five RADIUS servers can be configured.

If a server is unreachable, it is not used again by the RADIUS application until 30 seconds have elapsed, to give the server time to recover from its unreachable state. After 30 seconds, the unreachable server becomes available again for the RADIUS application.

If, within the 30 seconds, the RADIUS server receives a valid response to a previously sent RADIUS packet on that unreachable server, the server immediately becomes available again.

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+ 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.

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 7705 SAR does not require the configuration of VSAs (vendor-specific attributes) on the RADIUS server. However, users, user access permissions, and command authorization profiles must be configured on each router.

Any combination of these authentication methods can be configured to control network access from a 7705 SAR router:

- Local authentication
- RADIUS authentication
- TACACS+ authentication

3.1.1.1 Local authentication

Local authentication uses PKI or usernames and passwords configured on the router 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.

Remote security servers such as RADIUS or TACACS+ are not enabled.

3.1.1.1.1 Password hashing

The 7705 SAR supports two algorithms for user password hashing: bcrypt, which is the default algorithm, and PBKDF2. The PBKDF2 algorithm uses the SHA-2 and SHA-3 sets of cryptographic hash functions for password hashing.

A system administrator can change the default bcrypt password hashing algorithm to the PBKDF2 algorithm using the **config>system>security>password>hashing** command.

When the password hashing algorithm is changed to PBKDF2 SHA-2 or PBKDF2 SHA-3, users must change their passwords using the **/password** command to use the new hashing algorithm. The system administrator must then perform an **admin>save** command to store the new user passwords in the system configuration file.

After a password hashing change, any user logging in to the system who did not update their password to use the new hashing algorithm will be prompted to enter their old password the next time they log in. When the password is entered successfully, the user is prompted to enter a new password that will be hashed using the new algorithm.

3.1.1.2 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 administrators 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.

3.1.1.2.1 RADIUS server selection

Up to five RADIUS servers can be configured. They can be selected to authenticate user requests in two ways, using either the direct method or the round-robin method. The default method is direct.

Direct

In direct mode, the first server, as defined by the **server-index** command, is the primary server. This server is always used first when authenticating a request.

Round-robin

In round-robin mode, the server used to authenticate a request is the next server in the list, following the last authentication request. For example, if server 1 is used to authenticate the first request, server 2 is used to authenticate the second request, and so on.

3.1.1.3 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 login password to an authentication server to determine whether access can be allowed to a 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.

3.1.2 Authorization

The 7705 SAR supports the following authorization methods to control the actions of specific users:

- Local authorization
- RADIUS authorization
- TACACS+ authorization

Authorization operates by applying a profile based on username and password configurations after network access is granted. For RADIUS authorization, the profiles are configured locally on the router or downloaded using VSAs from a RADIUS server. For TACACS+ authorization, local profiles configured on the router can be used or remote profiles configured on the TACACS+ server can be used where each command is sent to the TACACS+ server for authorization. See RADIUS VSAs and TACACS+ services and VSAs.

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

TACACS+ separates the authentication and authorization functions. RADIUS combines the authentication and authorization functions.

3.1.2.1 Local authorization

Local authorization uses user profiles and user access information after a user is authenticated. The profiles and user access information specify the actions the user is allowed to perform.

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

You must configure profile and user access information locally.

3.1.2.2 RADIUS authorization

RADIUS authorization grants or denies access permissions for a 7705 SAR router. Permissions include the use of FTP, Telnet, SSH (SCP and SFTP), and console access. When granting Telnet, SSH (SCP and SFTP), and console access to the 7705 SAR 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 to.

After a user has been authenticated using RADIUS (or another method), the 7705 SAR router can be configured to perform authorization. The RADIUS server can be used to:

- download the user profile to the 7705 SAR router
- send the profile name that the node should apply to the 7705 SAR router
- control file access using VSAs (see RADIUS VSAs)

If RADIUS authentication is successful and no authorization is configured for the user on the RADIUS server, local (router) authorization is attempted if it is configured using the **authentication-order** command. 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. The temporary profiles are only downloaded if the user authenticates via RADIUS. RADIUS-based authorization is not supported for users who authenticate locally or via TACACS+.

The following table lists the supported authorization configurations.

Table 2: Supported authorization configurations

User	Local authorization	RADIUS authorization
7705 SAR configured user	✓	
RADIUS server configured user	✓	✓
TACACS+ server configured user	✓	

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.

3.1.2.3 TACACS+ authorization

Like RADIUS authorization, TACACS+ grants or denies access permissions for a 7705 SAR router. The TACACS+ server sends a response based on the username and password.

TACACS+ command authorization operates in the following ways:

- All users who authenticate via TACACS+ can use a single common command authorization profile that is configured locally on the router.

- Every command that a user attempts is sent to the TACACS+ server for authorization.
- The TACACS+ default template can be configured (**tacplus_default**) and vendor-specific attributes (VSAs) can be used to control file access. The **use-default-template** command must be enabled to configure all other access parameters locally. See TACACS+ services and VSAs for more information.

To use a single common default command authorization profile to control command authorization for TACACS+ users, enable the TACACS+ default user template and configure the template to point to a valid local profile. The local profile is then used for command authorization. TACACS+ authorization must be disabled.

CLI syntax:

```
config>system>security
    tacplus
        use-default-template
        no authorization
     user-template tacplus_default
        profile user-profile-name
```

When the **tacplus authorization** command is enabled, each CLI command that the user issues is sent to the TACACS+ server for authorization. The authorization request contains the first word of the CLI command as the value for the TACACS+ command and all following words as a command argument. Quoted values are expanded so that the quotation marks are stripped off and the enclosed values are seen as one command or command argument.

3.1.3 Accounting

Accounting tracks user activity to a specific host. The 7705 SAR supports RADIUS and TACACS+ accounting.

3.1.3.1 RADIUS accounting

When enabled, RADIUS accounting sends command line accounting from the 7705 SAR 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.

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 7705 SAR 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.

3.1.3.2 TACACS+ accounting

The 7705 SAR 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 will be sent or just stop packets will be sent. A start packet is sent to a TACACS+ server when an authenticated user establishes a Telnet or SSH session and a stop packet is sent when the user logs out.

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 7705 SAR 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, the device sends a start packet to the TACACS+ accounting server that 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.

3.2 Security controls

You can configure the 7705 SAR to use RADIUS, TACACS+, and local authentication to validate users requesting access to the network. The order in which requests are processed among RADIUS, TACACS+ and local methods can be specifically configured. For example, the authentication order can be configured to process authorization using TACACS+ first, then RADIUS, for authentication and accounting. Local access can be specified next in the authentication order if the RADIUS and TACACS+ servers are not operational.

3.2.1 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 if the primary server is responsive again are 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. If a server has the health check feature enabled and is unresponsive, the server’s status is checked every 30 seconds. Health check is enabled by default. When a service response is restored from at least one server, the alarm condition is cleared. Alarms are raised and cleared on 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 from a lower indexed server. If a response from the server is received, no other server is queried.

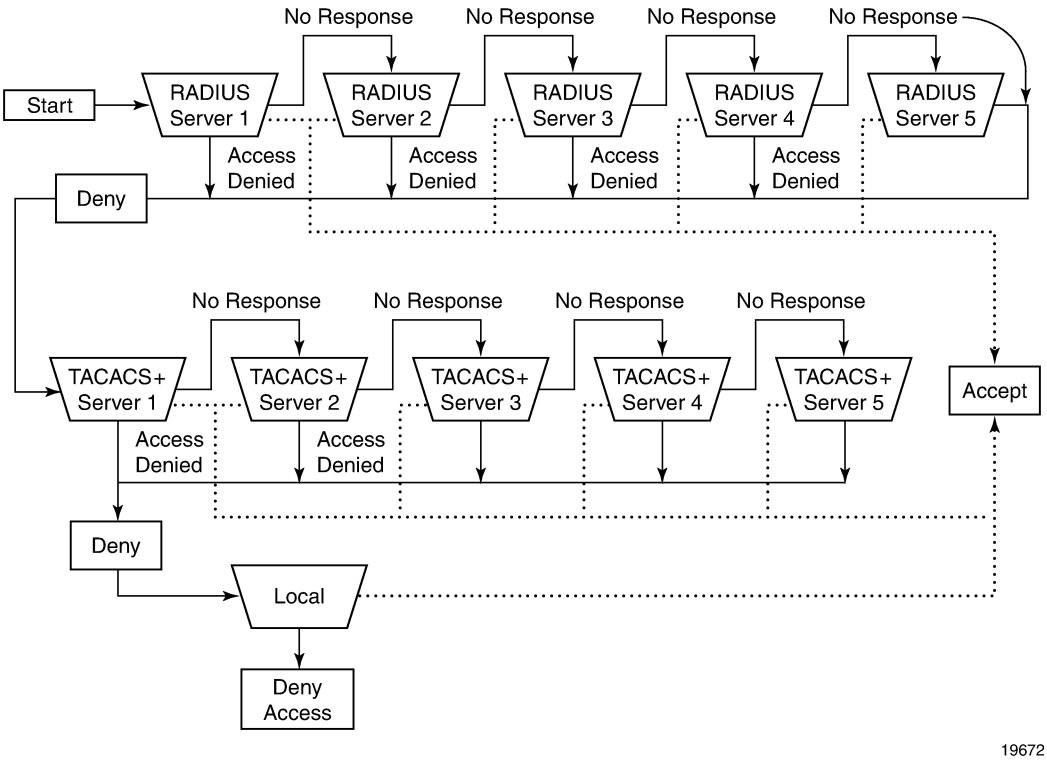
3.2.2 Authentication and authorization request flow

In Figure 2: Security flow, the authentication process is defined in the **config>system>security> password** context with the **authentication-order** command. The authentication order is determined by specifying the sequence in which password authentication is attempted among RADIUS, TACACS+, and local servers when **exit-on-reject** is disabled.

This example uses the authentication order of RADIUS, then TACACS+, and finally, local. A request is sent to RADIUS server 1. If there is no response from the server, the request is passed to the next RADIUS server, and so on, until the last RADIUS server is attempted (RADIUS server 5). If server 5 does not respond, the request is passed to TACACS+ server 1. If there is no response from that server, the request is passed to the next TACACS+ server, and so on.

If a request is sent to an active RADIUS server and the username and password are not recognized, access is denied and the next method is attempted, in this case, the TACACS+ server. The process continues until the request is accepted or denied or each server is queried. Finally, if the request is denied by the active TACACS+ server, the local method is attempted. This is the last chance for the access request to be accepted.

Figure 2: Security flow



3.3 RADIUS VSAs

The 7705 SAR supports the configuration of Nokia-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are defined in RFC 2138. If VSAs are not configured on the RADIUS server, the RADIUS user authenticates with options defined in the RADIUS default template when **use-default-template** is enabled. If VSAs are used, all mandatory VSAs must be configured for the RADIUS user to authenticate. 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. Nokia VSAs are defined in the dictionary-freeradius.txt file in the support folder of the software package.

Nokia supports the following RADIUS VSAs for AAA:

- **Timetra-Access <ftp> <console> <both> <scp-sftp> <console-port-cli> <ssh-cli> <telnet-cli>** – specifies the router management access methods a user can access. Multiple access methods can be specified by adding the value of the access methods to allow in the RADIUS server configuration file. This VSA is mandatory when the RADIUS default template is disabled.

  For example, to allow console port CLI and SSH CLI access:

  RADIUS server configuration

  ```
  Timetra-Access = 96 # 32 (console-port-cli) + 64 (ssh-cli)
  ```

  or

  ```
  Timetra-Access = console-port-cli
  Timetra-Access += ssh-cli
  ```

- **Timetra-Profile <profile-name>** – maps to the user profile, which must be configured on the 7705 SAR router. The following guidelines apply 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 7705 SAR router.
  - The user must be authenticated by the RADIUS server.
  - Up to eight 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 of the preceding conditions are not met, access to the router is denied and a failed login event or trap is written to the security log.
- **Timetra-Action <permit | deny>** – specifies the action to be applied when the user has entered a command specified in the **Timetable-Cmd** VSA
- **Timetra-Default-Action <permit-all | deny-all | read-only-all | none>** – 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. This VSA is mandatory when the RADIUS default template is disabled.
- **Timetra-Cmd <match-string>** – configures a command or command subtree as the scope for the match condition. The command and all commands in the subtrees are authorized. If an invalid command is specified, a **deny-all** profile is installed and the radiusUserProfileInvalid event is logged.
- **Timetra-Home-Directory <home-directory-string>** – specifies the home directory. It cannot be used to delete a home directory that is configured in the RADIUS default template.

- **Timetra-Restrict-To-Home <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-Save-When-Restricted <true | false>** – when this VSA is set to true, the user can execute configuration save operations (for example, **admin save**) in the CLI when **Timetra-Restrict-To-Home** is set to true.
- **Timetra-Exec-File <login-exec-string>** – specifies the login exec file that is executed when the user successfully logs in to a console session. If this VSA is not configured, no login exec file is applied.

3.3.1 RADIUS configuration for file access control using VSAs

File access control can be configured in one of the following ways depending on the file access requirements of users:

- locally with no VSAs (see Configuring users for information about configuring user access parameters locally)
- with VSAs

Note: File access is denied when the **restricted-to-home** command is configured unless the **home-directory** command is configured and the directory has been created by an administrator.

Example: RADIUS server with VSA configuration for per-user home directories and a locally configured default template for other options

This example shows the following configuration:

- all users can save the configuration
- on the router: each user has a home directory with restricted file access. The administrator must create the home directory for each user.
- on the RADIUS server: the home directory is configured with a VSA
- on the router: optionally, access to copy files to the router with SCP/SFTP is configured in the RADIUS default template
- on the router: other file access controls are configured in the RADIUS default template

RADIUS server configuration

```
user1
    Timetra-Home-Directory = "cf3:\users\user1"

user2
    Timetra-Home-Directory = "cf3:\users\user2"

user3
    Timetra-Home-Directory = "cf3:\users\user3"

user4
    Timetra-Home-Directory = "cf3:\users\user4"
```

CLI configuration

```
A:node-2>config>system>security>user-template# info
----------------------------------------------
restricted-to-home
```

```
save-when-restricted
-----------------------------------------------
```

Example: RADIUS server with VSA configuration and per-user home directories

This example shows the following configuration:

- all file access controls are configured with VSAs, which is the most flexible way to grant different file access to each user
- on the RADIUS server: each user has a home directory with restricted file access. The administrator must create the home directory for each user.
- on the router: the RADIUS default template is not used for file access
- on the RADIUS server: the administrator can restrict file access to the home directory of the user and allow users to save the configuration based on the VSA value
- on the RADIUS server: access to the router and permission to copy files to the router with SCP/SFTP are configured with VSAs

RADIUS server configuration – user1 has access to all files and can save the configuration and copy files to the router with SCP/SFTP:

```
user1
    Timetra-Access = 112 # 16 + (scp-sftp) + 32 (console-port-cli) + 64 (ssh-cli)
    # Timetra-Home-Directory is not defined
    Timetra-Restrict-To-Home = false
    # Timetra-Save-When-Restricted is not defined
```

RADIUS server configuration – user2 has home directory access and can save the configuration and copy files to the router with SCP/SFTP:

```
user2
    Timetra-Access = 112 # 16 + (scp-sftp) + 32 (console-port-cli) + 64 (ssh-cli)
    Timetra-Home-Directory = "cf3:\users\user2",
    Timetra-Restrict-To-Home = true,
    Timetra-Save-When-Restricted = true
```

RADIUS server configuration – user3 has home directory access but cannot save the configuration or copy files to the router with SCP/SFTP:

```
user3
    Timetra-Access = 96 # 32 (console-port-cli) + 64 (ssh-cli)
    Timetra-Home-Directory = "cf3:\users\user3",
    Timetra-Restrict-To-Home = true,
    Timetra-Save-When-Restricted = false
```

RADIUS server configuration – user4 has no file access and cannot save the configuration:

```
user4
    Timetra-Access = 96 # 32 (console-port-cli) + 64 (ssh-cli)
    # Timetra-Home-Directory is not defined
    Timetra-Restrict-To-Home = true,
    Timetra-Save-When-Restricted = false
```

3.4 TACACS+ services and VSAs

The 7705 SAR supports the "nokia-user" service with several VSAs. Administrators can optionally configure the service and VSAs for each user on a TACACS+ server instead of configuring access locally.

When a user authenticates with TACACS+, the router:

- if enabled, requests the "nokia-user" VSA from the server for authorization after authentication succeeds
- uses the values from the VSA if present and values from the TACACS+ default template when a VSA is not present
- discards invalid VSA values and authentication fails
- discards unknown VSAs and authentication succeeds
- discards unknown mandatory VSA values and authentication succeeds

The administrator must ensure that the **use-default-template** command is enabled so that users can be authenticated. If the default template (**tacplus_default**) is not enabled, no login access (FTP or console) will be granted because that access can only be configured via the default template (not through VSAs).

The following table describes the supported services and VSAs.

Table 3: TACACS+ VSAs

Service name	VSA name	Description	Values
nokia-user	**home-directory**	Home directory for the user	A string up to 200 characters
nokia-user	**restricted-to-home**	Limits user access to their home directory	true – prevents the user from accessing files outside their home directory false – allows the user to access all files on the system
nokia-user	**save-when-restricted**	Saves configurations when the user is restricted to home	true – allows all configuration save operations (for example, **admin save**) via the CLI even if **restricted-to-home** is enabled false – prevents the user from performing any configuration save operations outside of their home directory when **restricted-to-home** is enabled

3.4.1 TACACS+ configuration for file access control using VSAs

File access control can be configured in one of the following ways depending on the file access requirements of users:

- locally with no VSAs (see Configuring users for information about configuring user access parameters locally)
- locally using the TACACS+ default template (**tacplus_default**) and some VSAs that are different for each user
- using the file access VSAs to control file access and the TACACS+ default template for other user access controls

Note: File access is denied when the **restricted-to-home** command is configured unless the **home-directory** command is configured and the directory has been created by an administrator.

Note: If the home directory in the server configuration file (`tac_plus.conf`) is in quotation marks, you must add a backslash (\) to escape the backslash (\); otherwise, the TACACS+ server will reject the setting and fail to start. For example:

- **home-directory = cf3:\users\user1**
- **home-directory = "cf3:\\users\\user1"**

Note: Currently, user access cannot be defined on the TACACS+ server. Therefore, the TACACS + default template is the only place where this can be defined. This means that **use-default-template** must be enabled; otherwise, a mandatory attribute will be missing.

Example: TACACS+ server with VSA configuration for per-user home directories and a locally configured default template for other options

This example shows the following configuration:

- all users can save the configuration
- on the router: each user has a home directory with restricted file access. The administrator must create the home directory for each user.
- on the TACACS+ server: the home directory is configured with a VSA
- on the router: **use-default-template** is enabled under the **config>system>security>tacplus** context; this configuration is mandatory (see note above)
- on the router: other file access controls are configured in the TACACS+ default template

TACACS+ server configuration

```
user = user1 {
    service = nokia-user {
        home-directory = cf3:\users\user1
    }
}
user = user2 {
    service = nokia-user {
        home-directory = cf3:\users\user2
    }
}
user = user3 {
    service = nokia-user {
```

```
        home-directory = cf3:\users\user3
    }
}
user = user4 {
    service = nokia-user {
        home-directory = cf3:\users\user4
    }
}
```

CLI configuration

```
A:node-2>config>system>security>user-template# info
----------------------------------------------
restricted-to-home
save-when-restricted
----------------------------------------------
```

Example: TACACS+ server configuration with VSA configuration and per-user home directories

This example shows the following configuration:

- all file access is controlled with VSAs, which is the most flexible way to grant different file access to each user
- on the router: each user has a home directory with restricted file access. The administrator must create the home directory for each user.
- on the router: the TACACS+ default template is not used for file access
- on the TACACS+ server: the administrator can also restrict file access to the home directory of the user and allow users to save the configuration based on the VSA value

TACACS+ server configuration – user1 has access to all files and can save the configuration:

```
user = user1 {
    service = nokia-user {
        # home-directory is not defined
        restricted-to-home = false
        # save-when-restricted is not defined
    }
}
```

TACACS+ server configuration – user2 has home directory access and can save the configuration:

```
user = user2 {
    service = nokia-user {
        home-directory = cf3:\users\user2
        restricted-to-home = true
        save-when-restricted = true
    }
}
```

TACACS+ server configuration – user3 has home directory access but cannot save the configuration:

```
user = user3 {
    service = nokia-user {
        home-directory = cf3:\users\user3
        restricted-to-home = true
        save-when-restricted = false
    }
}
```

TACACS+ server configuration – user4 has no file access and cannot save the configuration:

```
user = user4 {
    service = nokia-user {
       # home-directory is not defined
        restricted-to-home = true
        save-when-restricted = false
    }
}
```

3.5 Other security features

This section contains information about the following topics:

- SSH
- CSM filters and CSM security
- Exponential login backoff
- File access controls
- Encryption
- 802.1x network access control
- TCP enhanced authentication and keychain authentication

3.5.1 SSH

Secure Shell (SSH) is a protocol that provides a secure, encrypted Telnet-like connection to a router.

A connection is always initiated by the client (the user). Authentication takes place by one of the configured authentication methods (local, RADIUS, or TACACS+). With authentication and encryption, SSH allows for a secure connection over an insecure network.

The 7705 SAR supports Secure Shell version 2 (SSHv2). SSHv2 uses host keys to authenticate systems 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 7705 SAR has a global SSH server process to support inbound SSH, SFTP, and SCP sessions initiated by external SSH or SCP client applications. The SSH server supports SSHv2. This server process is separate from the SSH and SCP client commands on the 7705 SAR, which initiate outbound SSH and SCP sessions.

Inbound SSH, Telnet, and FTP sessions are counted separately and it is possible to set the limit for each session type individually with the **config>system>login-control** command. However, there is a maximum of 50 sessions for SSH and Telnet together. SCP and SFTP sessions are counted as SSH sessions.

When the SSH server is enabled, an SSH security key is generated. Unless the **preserve-key** command is enabled, the key is only valid until either the node is restarted or the SSH server is stopped and restarted. The key size is non-configurable and is set to 2048 for SSHv2 RSA and to 1024 for SSHv2 DSA. Only SSHv2 RSA is supported in FIPS-140-2 mode. When the server is enabled, all inbound SSH, SCP, and SFTP sessions are accepted provided the session is properly authenticated.

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

When using SCP to copy files from an external device to the file system, the 7705 SAR SCP server will accept either forward slash (/) or backslash (\) characters to delimit directory and filenames. Similarly, the 7705 SAR 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 does not get transmitted to the 7705 SAR SCP server. For example, a destination directory specified as "cf3:\dir1\file1" will be transmitted to the 7705 SAR SCP server as "cf3:dir1file1", where the backslash escape characters are stripped by the SCP client system before transmission. On systems where the client treats the backslash like an "escape" character, a double backslash (\\) or the forward slash (/) can typically be used to properly delimit directories and the filename.

The 7705 SAR support for SSH, SCP, and SFTP is the same for both IPv4 and IPv6 addressing, including support for:

- SSHv2
- in-band and out-of-band management of the 7705 SAR
- key management and authentication types
- encryption types
- simultaneous IPv4 and IPv6 SSH/SCP/SFTP sessions

The 7705 SAR supports configurable lists for the following: cipher, key exchange (KEX) algorithms, and message authentication code (MAC) algorithms. These lists can be configured for an SSH client or an SSH server and are used to negotiate the best compatible cipher, KEX, or MAC algorithm between the client and server. The lists are created and managed under the **config>system>security>ssh** context. The client list is used when the 7705 SAR is acting as an SSH client and the server list is used when the 7705 SAR is acting as an SSH server.

3.5.1.1 SSH and Telnet listening ports configurable to a non-default value

For security reasons, the SSH server and Telnet server listening ports are configurable to a non-default port value. This configuration makes it more difficult for unauthorized users to scan the SSH or Telnet ports and launch Denial of Service (DoS) attacks. The 7705 SAR SSH and Telnet clients are capable of initiating an SSH or Telnet connection to a specific non-default SSH or Telnet port.

3.5.1.1.1 Ensuring no other application is using the SSH or Telnet port

When a user attempts to configure a new value for the default SSH or Telnet port, the SSH or Telnet application checks whether the port is in use by another protocol. If the port is in use, the configuration is blocked and a warning displays stating: "Port is already in use".

The newly configured port cannot be overwritten by any other protocol even if there is no active SSH or Telnet session. After the port is configured, no other protocol is allowed to reserve the port.

3.5.1.1.2 Behavior in base routing and VPRN

The 7705 SAR uses GRT leaking and the **allow-management** command for VPRN management. If the listening port for SSH or Telnet is changed, the configuration also applies to VPRN GRT leaking.

3.5.1.1.3 Known limitations

When SSH or Telnet in-band or out-of-band connections to the initial port exist, the port change back to the initial value is blocked until all connections to the initial port are closed. If the port is changed and there are open connections to the changed port, the connections must be closed manually to be able to revert to the previous port. For example:

- SSH is connected to port 22 and the user changes the port to 22000; the change is effective immediately, but the SSH connection to port 22 remains open.
- The port cannot be changed back from 22000 to 22 until all connections to port 22 are closed.

3.5.1.2 Multichannel SSH

The 7705 SAR supports up to five channels within a single SSH connection, up to a maximum of 15 channels per system. SSH channels can be used when an SSH connection has authenticated a user and a channel is opened for configuration while another channel is required to retrieve state information, such as collecting configurations or show command output. The primary connection authenticates the user through public key authentication (PKI) or keyboard authentication. After the primary connection is authenticated, applications can open multiple channels (sessions) to the server with the same connection.

Opening a new channel inside an existing authenticated SSH connection reduces the additional time and memory requirements for establishing a new SSH session. Reducing the time and memory needed is useful when, for example, multiple RPCs from different network managers to the same device are executed at the same time.

Note: Multiple channels are only supported for SSH and some applications that use SSH as transport. Multiple channels are not supported for SFTP or SCP.

3.5.1.3 SSH session closing behavior

The SSH connection closes automatically when the last channel (session) opened in the connection is closed.

SSH keepalive intervals are disabled on the 7705 SAR, which results in the following:

- the 7705 SAR SSH server does not close the session when the client SSH keepalive intervals time out
- the client SSH keepalive intervals cannot be used to keep the connection to the 7705 SAR server open

3.5.1.4 SSH PKI authentication

The SSH server supports public key authentication (also known as PKI) if the server has been previously configured to know the client's public key.

Using public key authentication can be more secure than the existing username and password method for the following reasons:

- 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. Therefore, the password is less likely to be compromised.

The 7705 SAR supports server-side SSHv2 public key authentication but does not include a key-generation utility.

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

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

3.5.1.4.1 User public key generation

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

The 7705 SAR currently supports Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys. The RSA public key is supported up to 4096 bits and the ECDSA public key is supported up to NIST P-521.

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

Next, the public key must be configured for the user on the 7705 SAR with the command **config>system>security>user>public-keys**. The user can program the public key using the CLI or SNMP.

3.5.1.5 SSH cipher lists

The 7705 SAR supports configurable cipher client and cipher server lists that are used to negotiate the best compatible cipher between the SSH client and SSH server. Each list contains ciphers and their corresponding index values, where a lower index has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their cipher lists, the first cipher in the client list that is also supported by the server is the cipher that is agreed upon.

See Table 11: SSHv2 default index values in the Security command reference for the cipher index values and names.

The default list can be changed by manually removing a single index or as many indexes as required using the **no cipher** *index* command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required (the 7705 SAR does not support customizing an index without first removing it).

3.5.1.6 SSH KEX lists

The 7705 SAR supports configurable KEX client and KEX server lists that are used to negotiate the best compatible KEX algorithm between the SSH client and SSH server. Each list contains KEX algorithms

and their corresponding index values, where a lower index value has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their KEX lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon.

The KEX client and KEX server each have a default list that contains all supported algorithms and their corresponding indexes. See Table 12: Default KEX index values in the Security command reference for the default KEX index values and algorithms.

The default list can be changed by manually removing a single index or as many indexes as required using the **no kex** *index* command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required (the 7705 SAR does not support customizing an index without first removing it).

Once a change has been made to the default list, the 7705 SAR uses the changed list moving forward. To go back to using the hard-coded list, the default KEX indexes must be manually re-entered with their corresponding algorithms. If all the entries in a KEX list are removed, the list will be empty and any KEX algorithm brought to the negotiation will be rejected.

3.5.1.7 SSH key re-exchange without disabling SSH

The 7705 SAR supports periodic rollover (or re-exchange) of the SSH symmetric key without disabling SSH. Symmetric key rollover is important in long SSH sessions. Symmetric key rollover ensures that the encryption channel between the client and server is not jeopardized by an external hacker that is trying to break the encryption via a brute force attack. The feature can be configured on either the SSH client or server.

The following are triggers for symmetric key rollover and negotiation:

- the negotiation of the key based on a configured time period
- the negotiation of the key based on a configured data transmission size

Key re-exchange is enabled by default. The default values for both the client and server are 60 min and 1024 MB, which is the RFC 4253 recommendation.

3.5.1.7.1 Key re-exchange procedure

The key re-exchange procedure is initiated by sending an SSH_MSG_KEXINIT message while not performing a key exchange. When this message is received by a client or server, the client or server must respond with its own SSH_MSG_KEXINIT message, except in cases where the received SSH_MSG_KEXINIT message was already sent as a reply. Either client or server can initiate the re-exchange, but the roles must not be changed (that is, the server must remain the server and the client must remain the client).

Key re-exchange is performed using whatever encryption was in effect when the exchange was initiated. Encryption, compression, and MAC methods are not changed before a new SSH_MSG_NEWKEYS message is sent after the key exchange (as in the initial key exchange). Re-exchange is processed in the same way as the initial key exchange, except that the session identifier remains unchanged. Some or all of the algorithms can be changed during the re-exchange. Host keys can also change. All keys and initialization vectors are recomputed after the exchange. Compression and encryption contexts are reset.

Note: If the key re-exchange parameters are modified, only new SSH connections inherit the new parameters. The existing SSH connections use the previously configured parameters.

3.5.1.8 SSH MAC lists

The 7705 SAR supports configurable SSHv2 server MAC and client MAC lists that are used to negotiate the best compatible MAC algorithm between the SSH client and SSH server.

Each list contains MAC algorithms and their corresponding index values, where a lower index value has a higher preference in the SSHv2 negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their MAC lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon.

In addition, strong HMAC algorithms can be configured at the top of the MAC list (that is, as the lowest index values in the list) in the order 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.

The default list can be changed by manually removing a single index or as many indexes as required using the **no mac** *index* command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required (the 7705 SAR does not support customizing an index without first removing it).

3.5.1.9 SFTP

When an SSH server is enabled on the 7705 SAR, users can connect to the node through SSH File Transfer Protocol (SFTP). SFTP runs on top of SSH and uses the same password and authentication process, and once logged in, SFTP users will appear as regular SSH users. Additionally, all other user management features apply to users logging in to the 7705 SAR with an SFTP client.

Event logs are created to capture both successful and unsuccessful attempts to access the node through SFTP.

3.5.2 CSM filters and CSM security

IP forwarding supports CSM filters that are applied to IP packets extracted to the control plane. CSM filters are used to protect the control plane from DoS attacks, unauthorized access to the node, and similar security breaches.

IP filters scan all traffic and take the appropriate (configured) action against matching packets. Packets that are not filtered by the IP filters and are destined for the 7705 SAR are scanned by the configured CSM filter.

For information about IP filters, see the 7705 SAR Router Configuration Guide.

Note: Although the Control and Switching module on the 7705 SAR is called a CSM, the CSM filters are referred to as CPM filters in the CLI to maintain consistency with other SR routers.

Both IPv4 and IPv6 CSM filters are supported.

IPv4 CSM filters drop or accept incoming packets based on the following match criteria:

- DSCP name
- destination IP address
- destination port
- fragmentation

- ICMP code
- ICMP type
- IP option value
- multiple options
- option present
- source IP address
- source port
- TCP ACK
- TCP SYN

IPv6 CSM filters drop or accept incoming packets based on the following match criteria:

- DSCP name
- destination IP address
- destination port
- ICMP code
- ICMP type
- source IP address
- source port
- TCP ACK
- TCP SYN

To prevent DoS-like attacks from overwhelming the control plane while ensuring that critical control traffic such as signaling is always serviced in a timely manner, the 7705 SAR segregates the incoming control plane traffic into different queues. These queues are used to shape and rate-limit traffic for each protocol or group of protocols, or on a per-flow basis, with the main goal of mitigating DoS attacks and ensuring that the control plane does not end up with more traffic than it can handle.

These queues are fixed use (each queue handles a specific type of traffic, which is not user-configurable) and fixed configuration (each queue is configured for particular rates and buffering capacity and is not user-configurable).

3.5.3 Exponential login backoff

A malicious user can gain CLI access via a dictionary attack: using a script to try "admin" with any password.

The 7705 SAR increases the delay between login attempts exponentially to mitigate attacks. It is applied to the console login. SSH and Telnet sessions terminate after four attempts.

3.5.4 File access controls

Files on the 7705 SAR can be accessed locally using the CLI **file** commands and output modifiers, such as > (file redirect), or remotely via FTP or SCP. The 7705 SAR can control file access to:

- allow users to access all files and save the configuration

- allow users to access only the files in their home directory and save the configuration
- allow users to access only the files in their home directory with no ability to save the configuration
- prevent users from accessing any files or saving the configuration

The file access controls provide different levels of user access. File access controls can also be configured to allow users to save the configuration to a system file that is stored outside their home directory when their file access is restricted to their home directory. A home directory is typically a working space for the user; for example, cf3:\users\user1. Although the home directory can be configured to contain saved configuration files, log files, or other system files, administrators should only do this for users who are intended to have access to those files.

The following commands configure file access controls for local or remote users; these commands can be set via the CLI, RADIUS VSAs, or TACACS+ VSAs:

- **restricted-to-home** – limits file access to only the files in the home directory of the user
- **home-directory** – home directory for the user; Nokia recommends that this command not be configured in the RADIUS or TACACS+ default template because each user should have their own home directory
- **save-when-restricted** – allows the user to save configurations when the user is restricted to their home directory, even if the saved configuration file is outside the home directory of the user

High-privilege users and administrators have access to the router configuration file via the CLI, SCP, and SFTP, and must be trusted. Medium-privilege and low-privilege users with access to a subset of the configuration must be configured with **restricted-to-home** and a **home-directory** to restrict their access to the file system via the CLI, SCP, and SFTP. The home directory must not contain the saved configuration file.

Note: The **restricted-to-home** configuration is the default setting for non-administrative users. For administrative users (**user "admin"**), the default is **no restricted-to-home**.

The following table lists the user types and privileges and their corresponding file access control configuration.

Table 4: File access control configuration

Type of user	File system access	Configuration access	Restricted to home	Home directory	Save when restricted
High-privilege administrator	Full	Yes	Disabled (false)	Unconfigured	Unconfigured
High-privilege user with access to all configuration	Private directory with environment settings and Python applications	Yes	Enabled (true)	cf3:\users\user1	Enabled (true)
Medium-privilege user with access to a subset of configuration using AAA command authorization	Directory of CLI scripts and Python applications	Yes	Enabled (true)	cf3:\scripts\script-group-a	Enabled (true)

Type of user	File system access	Configuration access	Restricted to home	Home directory	Save when restricted
Medium-privilege user with access to a subset of configuration using AAA command authorization	None	Yes	Enabled (true)	Unconfigured	Enabled (true)
Low-privilege operational user	Private directory with environment settings and operational scripts	No	Enabled (true)	cf3:\users\user2	Unconfigured[1]
Low-privilege operational user	None	No	Enabled (true)	Unconfigured	Unconfigured[1]
Low-privilege user for managing XML accounting files	Accounting directory	No	Enabled (true)	cf2:\act	Unconfigured[1]
Low-privilege user for managing log files	Log directory	No	Enabled (true)	cf2:\log	Unconfigured[1]

Note:

1. Configuration save operations (for example, **admin save**) are controlled by AAA command authorization. Optionally, **save-when-restricted** can be disabled to explicitly deny configuration save operations for these user types.

The following examples show how to use the CLI to configure different permissions for local users. The administrator must create a home directory for each user.

Example: access to all files and the ability to save the configuration

Use the following configuration for a high-privilege administrator who needs access to all files:

```
config>system>security
             user user1
                 no restricted-to-home
```

Example: access to home directory files only and the ability to save the configuration

Use the following configuration for a medium-privilege user who can access some parts of the configuration and needs to save the configuration, but is denied access to other parts of the configuration in a AAA profile:

```
config>system>security
             user user2
             home-directory "cf3:\users\user2"
             restricted-to-home
             save-when-restricted
```

Example: access to home directory files only and no ability to save the configuration

Use the following configuration for a low-privilege user who does not have access to any part of the configuration but still requires a working area on the file system for their own files:

```
config>system>security
              user user3
              home-directory "cf3:\users\user3"
              restricted-to-home
              no save-when-restricted
```

Example: no file access and no ability to save the configuration

Use the following configuration for a low-privilege user who does not have access to any part of the configuration and does not require any file system access:

```
config>system>security
              user user4
              restricted-to-home
              no save-when-restricted
```

3.5.5 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.

3.5.6 802.1x network access control

The 7705 SAR 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.

See the 7705 SAR Interface Configuration Guide for more information about IEEE 802.1x.

3.5.7 TCP enhanced authentication and keychain authentication

The 7705 SAR supports non-keychain MD5 authentication for OSPF, IS-IS, and RSVP-TE and TCP MD5 authentication for BGP and LDP. In previous releases, only a single authentication key or pre-hashed MD5 digest could be defined at a time using the **authentication-key** command. If this key was changed, the adjacency was reset, causing both the local and remote router to reconverge based on the lost adjacency. When a new key or digest was added, the adjacency was re-established, causing another reconvergence event within the network.

The 7705 SAR also supports the TCP Enhanced Authentication Option, as specified in *draft-bonica-tcp-auth-05, Authentication for TCP-based Routing and Management Protocols*. The TCP Enhanced Authentication option is a TCP extension that enhances security for BGP, LDP, and other TCP-based protocols. It extends the MD5 authentication option to include the ability to change keys in a BGP or LDP session seamlessly without tearing down the session and allows for stronger authentication algorithms to

be used. It is intended for applications where secure administrative access to both endpoints of the TCP connection is normally available.

TCP peers can use this extension to authenticate messages passed between one another. This strategy improves upon the practice described in RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*. Using this 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.

3.5.7.1 Keychain authentication

TCP enhanced authentication uses keychains that are associated with every protected TCP connection.

The keychain concept supported by BGP and LDP has also been extended to the OSPF, IS-IS, and RSVP-TE protocols.

The keychain mechanism allows for the creation of keys used to authenticate protocol communications. Each keychain entry defines the authentication attributes to be used in authenticating protocol messages from remote peers or neighbors. The keychain must include at least one key entry to be valid. The keychain mechanism also allows authentication keys to be changed without affecting the state of the associated protocol adjacencies.

Each key within a keychain must include the following attributes for the authentication of protocol messages:

- key identifier – unique identifier, expressed as a decimal integer
- authentication algorithm – see Table 5: Security algorithm support per protocol
- authentication key – used by the authentication algorithm to authenticate packets
- direction – packet stream direction in which the key is applied (receive direction, send direction, or both)
- begin time – the time at which a new authentication key can be used

Optionally, each key can include the following attributes:

- end time – the time at which the authentication key becomes inactive (applies to received packets only)
- tolerance – period in which both old and new authentication key values can overlap and both keys are allowed on received packets (applies to received packets only)

For added security, support for the Secure Hash Algorithm (SHA) has been added. The following table lists the security algorithms supported per protocol.

Table 5: Security algorithm support per protocol

Protocol	Clear text	MD5 (message digest)	HMAC-MD5	HMAC-SHA-1-96	HMAC-SHA-1	HMAC-SHA-256	AES-128-CMAC-96
OSPF	✓	✓		✓	✓	✓	
IS-IS	✓		✓		✓	✓	
RSVP-TE			✓	✓	✓	✓	
BGP				✓			✓

Protocol	Clear text	MD5 (message digest)	HMAC-MD5	HMAC-SHA-1-96	HMAC-SHA-1	HMAC-SHA-256	AES-128-CMAC-96
LDP				✓			✓

3.5.7.2 Keychain configuration guidelines and behavior

- The **authentication-key** command or the **auth-keychain** command can be used by the protocols listed in Table 5: Security algorithm support per protocol, but both cannot be supported at the same time. If both commands are configured, the **auth-keychain** configuration is applied and the **authentication-key** command is ignored.
- A keychain cannot be referenced by a protocol until it has been configured.
- If a keychain is referenced by a protocol, the keychain cannot be deleted.
- If multiple keys in a keychain are valid at the same time, the newest key (key with the most current **begin-time**) is used.
- If a protocol sends a packet that is configured to use a keychain, the most current key from that keychain is used.
- If a protocol receives a packet that is configured to use a keychain, the current key set is returned to authenticate the received packet:
  - The key set includes the currently active keys (based on the current system time) and the **begin-time** or **end-time** associated with each key in the specified keychain.
  - If a tolerance value is set for a key, the key is returned as part of the key set if the current time is within the key's **begin-time**, plus or minus the tolerance value. For example, if the **begin-time** is 12:00 p.m. and the **tolerance** is 600 seconds, the new key is included from 11:55 a.m. and the key to be replaced is included until 12:05 p.m.
- The **end-time** and **tolerance** parameters apply only to received packets. Transmitted packets always use the newest key, regardless of the tolerance value.
- If a keychain exists but there are no active key entries with an authentication type that matches the type supported by the protocol, inbound protocol packets are not authenticated and are discarded and no outbound protocol packets are sent.
- If a keychain exists but the last key entry has expired, a log entry is raised indicating that all keychain entries have expired.
  - The OSPF and RSVP-TE protocols continue to authenticate inbound and outbound traffic using the last valid authentication key.
  - The IS-IS protocol does not revert to an unauthenticated state and requires that the old key not be used; therefore, when the last key has expired, all traffic will be discarded.

For information about associating keychains with protocols, see the 7705 SAR Routing Protocols Guide (for OSPF, IS-IS, and BGP), the 7705 SAR MPLS Guide (for RSVP-TE and LDP), and the 7705 SAR Services Guide (for OSPF and BGP in a VPRN service).

3.5.7.3 Key rollover

Use the following commands to configure keychain authentication to roll over to a new key without tearing down the session:

```
config>system>security
    keychain name
        direction
            uni
                receive
                    entry entry-id
                        begin-time [date] [hours-minutes] [UTC]
                        end-time [date] [hours-minutes] [UTC]
                send
                    entry entry-id
                        begin-time [date] [hours-minutes] [UTC]
            bi
                    entry entry-id
                        begin-time [date] [hours-minutes] [UTC]
```

The **begin-time** command specifies when the authentication key starts to authenticate the protocol stream and the **end-time** command specifies when the authentication key is no longer eligible to authenticate the protocol stream. The system uses the key configured with the most recent **begin-time**. For more information about configuring keychain authentication, see Configuring keychain authentication.

A user does not have to configure an **end-time** and can instead choose to configure multiple entries with different **begin-time** configurations so that the newest key (key with the most current **begin-time**) is used. The current key pair is replaced to improve security without session loss between two peers.

3.5.8 TLS

Transport Layer Security (TLS) is used for two primary purposes:

- authentication of an end device (client or server) using a digital signature (DS)
  TLS uses PKI for device authentication. DSs are used to authenticate the client or the server. The server typically sends a certificate with a DS to the client.

  In specific situations, the server can request a certificate from the client to authenticate it. The client has a certificate (called a trust anchor) from the certificate authority (CA) that is used to authenticate the server certificate and its DS. After the client provides a digitally signed certificate to the server and both parties are authenticated, the encryption PDUs can then be transmitted.
- encryption and authentication of application PDUs
  After the client and server have been successfully authenticated, the cipher suite is negotiated between the server and clients, and the PDUs are encrypted based on the agreed cipher protocol.

3.5.8.1 TLS interaction with applications

TLS is a standalone configuration. The user must configure a TLS client profile with certificates and trust anchors, and then assign the TLS client profile to the appropriate applications. When a TLS client profile is assigned to an application, the application does not send any PDUs until the TLS handshake has been successfully completed and the encryption ciphers have been negotiated between the TLS server and the TLS client.

After successful negotiation and handshake, the application is notified that TLS is operationally up. The application begins transmitting PDUs encrypted using TLS based on the agreed ciphers. If at any point the TLS becomes operationally down, the application will stop transmitting PDUs.

For example, a TLS connection with the PCEP application operates as follows:

1. A TLS client is configured under PCEP on the 7705 SAR.
2. PCEP stops sending clear text PDUs because a TLS client profile has been assigned and TLS is not ready to encrypt.
3. The TLS client begins the handshake.
4. Authentication occurs at the TLS layer.
5. The TLS server and TLS client negotiate ciphers.
6. Salts are negotiated for the symmetric key. A salt is a seed for creating AES encryption keys.
7. When negotiations are successfully completed, the handshake finishes, TLS becomes operationally up, and PCEP is notified.
8. PCEP begins transmitting PDUs that are encrypted using TLS.

Until TLS becomes operationally up, PCEP does not transmit any PDUs.

3.5.8.1.1 Application support

The 7705 SAR supports TLS client profiles on the PCC to enable PCEP over TLS (PCEPS). See the "PCEP over TLS" section in the 7705 SAR MPLS Guide for more information.

3.5.8.2 TLS handshake

The following figure shows the TLS handshake process and the table describes the steps.

Figure 3: TLS handshake

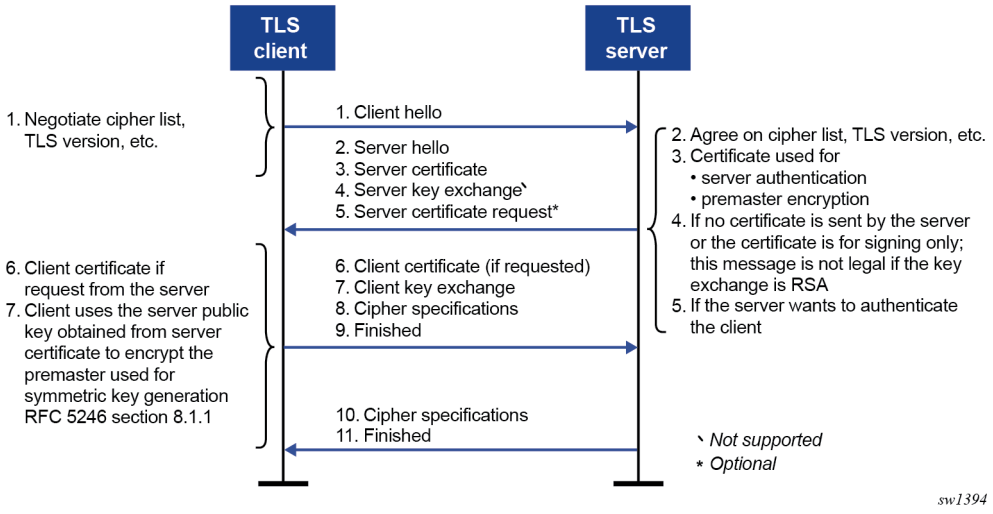


Table 6: TLS handshake steps

Step	Description
1	The TLS handshake begins with the client Hello message. This message includes the cipher list that the client wants to use and negotiate.
2	The TLS server sends back a server Hello message, along with the first common cipher found on both the client cipher list and the server cipher list. This agreed cipher is used for data encryption.
3	The TLS server continues by sending a server certificate message, where the server provides a certificate to the client so that the client can authenticate the server identity. The public key of this certificate (RSA key) can also be used for encryption of the symmetric key seed that is used by the client and server to create the symmetric encryption key. This occurs only if PKI is using RSA for asymmetric encryption.
4	Server key exchange is not supported by the 7705 SAR. The 7705 SAR only uses RSA keys; Diffie-Hellman key exchange is not supported.
5	The server can optionally be configured to request a certificate from the client to authenticate the client.
6	If the server requests a certificate, the client must provide a certificate using a client certificate message. If the client does not provide a certificate, the server drops the TLS session.
7	The client uses the server public RSA key that was included in the server certificate to encrypt a seed used for creating the symmetric key. This seed is used by the client and server to create the identical symmetric key for encrypting and decrypting the data plane traffic.
8	The client sends a cipher specification to switch encryption to this symmetric key.
9	The client successfully finishes the handshake.
10	The server sends a cipher specification to switch encryption to this symmetric key.
11	The server successfully finishes the handshake.

After a successful handshake, TLS is operationally up and can be used for application encryption.

3.5.8.3 TLS 1.3

TLS 1.3 is required for faster handshakes, stronger encryption, and authentication algorithms.

All 7705 SAR applications that use TLS 1.2 also support TLS 1.3, unless specifically stated otherwise.

The user can configure the node to use TLS 1.2, TLS 1.3, or both for negotiation.

If TLS 1.3 is negotiated with a peer, the node does not negotiate the TLS version down to 1.2 as long as the session is alive.

TLS 1.3 handshake

The TLS 1.3 client handshake is very similar to TLS 1.2 because the client is able to negotiate TLS 1.2 or 1.3 when starting the TLS Hello message to the server. The client includes a "Supported Version" extension in its Hello message. The server responds with its own supported version and agreed ciphers. The server and client must agree on the TLS version to proceed with the connection.

In TLS 1.2 and TLS 1.3, the server can optionally request the client certificate to authenticate the client. If requested, the client must provide its certificate to the server.

TLS 1.3 configuration

The user can configure the TLS 1.3 cipher list independently of TLS 1.2. TLS 1.3 ciphers are configured using the **tls13-cipher** command. When the user configures a TLS 1.3 cipher list, TLS 1.3 is included as a supported version in the TLS handshake.

TLS 1.3 also introduces group lists and signature lists for the server and client.

In the Hello message sent by the client, the "supported_groups" extension indicates the named groups that the client supports for the key exchange, ordered from most preferred to least preferred. TLS 1.3 supports Elliptic-curve Diffie-Hellman Ephemeral (ECDHE) groups.

Note: TLS 1.2 does not support Diffie-Hellman groups as an asymmetric key.

TLS 1.3 also allows the selection of signature algorithms. The "signature_algorithms_cert" extension is included to allow implementations that support different sets of algorithms for certificates and in TLS itself to clearly signal their capabilities.

3.5.8.4 TLS client certificate

The TLS protocol is used for authentication, and therefore the server can ask to authenticate the client via PKI. If the server requests authentication from the client, the client must provide an X.509v3 certificate to the server so that it can be authenticated via the digital signature of its client.

The 7705 SAR supports the configuration of an X.509v3 certificate for TLS clients.

When the server requests a certificate via the server’s Hello message, the client transmits its certificate to the server using a client certificate message.

3.5.8.5 TLS symmetric key rollover

The 7705 SAR supports key rollover when the TLS server is enabled with a TLS renegotiation timer and sends a HelloRequest message as specified in RFC 5246, section 7.4.1.1.

3.5.8.6 Supported TLS ciphers

As shown in Figure 3: TLS handshake, TLS negotiates the supported ciphers between the client and the server.

The client sends the supported cipher suites in the client Hello message, and the server compares them with the server cipher list. The top protocol on both lists is chosen and returned from the server in the server Hello message.

The 7705 SAR supports the following ciphers as a TLS 1.2 client:

- tls-rsa-with3des-ede-cbc-sha
- tls-rsa-with-aes128-cbc-sha
- tls-rsa-with-aes256-cbc-sha
- tls-rsa-with-aes128-cbc-sha256
- tls-rsa-with-aes256-cbc-sha256

The 7705 SAR supports the following TLS 1.3 ciphers, groups, and signature algorithms as a TLS 1.3 client:

- ciphers:
  - tls-aes128-gcm-sha256
  - tls-aes256-gcm-sha384
  - tls-chacha20-poly1305-sha256
  - tls-aes128-ccm-sha256
  - tls-aes128-ccm8-sha256
- groups:
  - tls-ecdhe-256
  - tls-ecdhe-384
  - tls-ecdhe-521
  - tls-x25519
  - tls-x448
- signature algorithms:
  - tls-rsa-pkcs1-sha256
  - tls-rsa-pkcs1-sha384
  - tls-rsa-pkcs1-sha512
  - tls-ecdsa-secp256r1-sha256
  - tls-ecdsa-secp384r1-sha384
  - tls-ecdsa-secp521r1-sha512
  - tls-rsa-pss-rsae-sha256
  - tls-rsa-pss-rsae-sha384
  - tls-rsa-pss-rsae-sha512
  - tls-rsa-pss-pss-sha256
  - tls-rsa-pss-pss-sha384
  - tls-rsa-pss-pss-sha512
  - tls-ed25519
  - tls-ed448

3.5.8.7 Certificate management

The 7705 SAR implements a centralized certificate management protocol that can be used by TLS. See the "IPSec" section in the 7705 SAR Services Guide for information about the configuration of the certificates and the corresponding protocols, such as OCSP and CRL.

3.5.8.7.1 Certificate profile

The certificate profile is available for the TLS client and is configured with the **cert-profile** command. The certificate profile contains the certificates that the client sends to the TLS server along with its DS so that the server can authenticate it via the **trust-anchor** and CA certificate.

Multiple provider certificates can be configured; however, the 7705 SAR currently uses the smallest index as the active provider certificate, and only sends that certificate to the server.

3.5.8.7.2 TLS server authentication of the client certificate CN field

If the client provides a certificate, the server checks the common name (CN) field against local CN configurations. The CN is validated via the client IPv4/IPv6 address or FQDN. If the common-name list authentication option is not enabled on the server, it uses certificate signature authentication instead.

3.5.8.8 Operational guidelines

3.5.8.8.1 Server authentication behavior

Following the Hello messages, the server sends its certificate in a certificate message if it is to be authenticated.

The **trust-anchor-profile** command determines whether the server must be authenticated by the client.

Note: If the **trust-anchor-profile** is configured and the **ca-profile** is missing from this **trust-anchor-profile**, the TLS connection fails and an "unknown_ca" error is generated, as per RFC 5246, section 7.2.2.

One of the following configurations can be used to establish server connectivity:

1. If **trust-anchor-profile** is configured under the TLS **client-tls-profile** context, the server must be authenticated via the **trust-anchor-profile** command before a trusted connection is established between the server and the client.
2. If there is no **trust-anchor-profile** under the **client-tls-profile** context, the trusted connection can be established without server authentication. The RSA key of the certificate is used for public key encryption, requiring basic certificate checks to validate the certificate. These basic checks are as follows:
   - **time validity**

     The certificate is checked to ensure that it is not expired or not yet valid.
   - **certificate type**

The certificate is not a CA certificate.

- **keyUsage extension**

  If present, this must contain a digital signature and key encryption.

- **host verification**

  The IP address or DNS name of the server is looked up, if available, in the common name (cn) or subjectAltName extension. This is to verify that the certificate was issued to that server and not to another.

3.5.8.8.2 TLS client profile and trust anchor behavior and scale

The 7705 SAR supports the creation of TLS client profiles, which can be assigned to applications such as PCEP to encrypt the application layer.

The **client-tls-profile** command is used for negotiating and authenticating the server. After the server is authenticated via the trust anchor profile (configured using the **trust-anchor-profile** command) of a TLS client profile, it negotiates the ciphers and authentication algorithms to be used for encryption of the data.

The TLS client profile must be assigned to an application for it to start encrypting. Up to 16 TLS client profiles can be configured. Because each of these client profiles needs a trust anchor profile to authenticate the server, up to 16 trust anchor profiles can be configured. A trust anchor profile holds up to 8 trust anchors (configured using the **trust-anchor** command), each of which holds a CA profile (**ca-profile**).

A CA profile is a container for installing CA certificates. These CA certificates are used to authenticate the server certificate. When the client receives the server certificate, it reads through the trust anchor profile CA certificates and tries to authenticate the server certificate against each CA certificate. The first CA certificate that authenticates the server is used.

3.5.8.9 Basic TLS configuration

Basic TLS client configuration must have a cipher list created using the **config>system>security>tls>client-cipher-list** command, and the cipher list must be assigned to the TLS client profile using the **config>system>security>tls>client-tls-profile>cipher-list** command.

TLS imports the trust anchor certificate for peer certificate authentication and public key retrieval. The following example shows a TLS configuration.

Example:

```
A:node-2>config>system>security>tls# info
----------------------------------------------
        trust-anchor-profile "server-1-ca" create
            trust-anchor "tls-server-1-ca"
        exit
        client-cipher-list "to-active-server" create
            cipher 1 name tls-rsa-with-aes256-cbc-sha256
            cipher 2 name tls-rsa-with-aes128-cbc-sha256
            cipher 3 name tls-rsa-with-aes256-cbc-sha
        exit
        client-tls-profile "server-1-profile" create
            cipher-list "to-active-server"
            trust-anchor-profile "server-1-ca"
            no shutdown
        exit
```

```
-----------------------------------------------
```

3.5.8.10 Common configuration tasks

3.5.8.10.1 Configuring a TLS client profile

The following displays the CLI syntax for a TLS client profile:

CLI syntax:

```
config>system>security>tls
    client-tls-profile name
        trust-anchor-profile name
```

3.5.8.10.2 Configuring a TLS client certificate

The following displays the CLI syntax for TLS certificate management:

CLI syntax:

```
config>system>security>tls
    cert-profile profile-name
        entry entry-id
            cert cert-filename
            key key-filename
            send-chain
                ca-profile name
            no shutdown
    client-tls-profile name
        cert-profile name
```

3.5.8.10.3 Configuring a TLS trust anchor

The following displays the CLI syntax for a TLS trust anchor:

CLI syntax:

```
config>system>security>tls
    trust-anchor-profile name
    client-tls-profile name
        cipher-list name
        no shutdown
        trust-anchor-profile name
```

The following example shows a TLS trust anchor configuration:

Example:

```

*A:node-2>config>system>security>tls# info
-----------------------------------------------
        trust-anchor-profile "server-1-ca" create
            trust-anchor "tls-server-1-ca"
        exit
        client-tls-profile "server-1-profile" create
```

```
            cipher-list "to-active-server"
            trust-anchor-profile "server-1-ca"
            no shutdown
        exit
```

3.6 Configuration notes

The following are security configuration guidelines and restrictions:

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

3.7 Configuring security with CLI

This section provides information to configure security using the command line interface. Topics in this section include:

- Setting up security attributes
- Security configurations
- Security configuration procedures

3.8 Setting up security attributes

The following table depicts the capabilities of authentication, authorization, and accounting configurations. For example, authentication can be enabled locally and on RADIUS and TACACS+ servers. Authorization can be executed locally, on a RADIUS server, or on a TACACS+ server. Accounting can be performed on a RADIUS or TACACS+ server.

Table 7: Security configuration requirements

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

3.8.1 Configuring authentication

See the following sections to configure authentication:

- local authentication
  - Configuring password management parameters

  - Configuring profiles
  - Configuring users
- RADIUS authentication (with local authorization)

  By default, authentication is enabled locally. Perform the following tasks to configure security on each participating 7705 SAR router:

  - Configuring profiles
  - Configuring RADIUS authentication
  - Configuring users
- RADIUS authentication (with RADIUS authorization)

  To implement RADIUS authentication with authorization, perform the following tasks on each participating 7705 SAR router:

  - Configuring RADIUS authentication
  - Configuring RADIUS authorization
- TACACS+ authentication

  To implement TACACS+ authentication, perform the following tasks on each participating 7705 SAR router:

  - Configuring profiles
  - Configuring users
  - Enabling TACACS+ authentication

3.8.2 Configuring authorization

See the following sections to configure authorization:

- local authorization

  For local authorization, configure these tasks on each participating 7705 SAR router:

  - Configuring profiles
  - Configuring users
- RADIUS authorization with authentication

  For RADIUS authorization with authentication, configure these tasks on each participating 7705 SAR router:

  - Configuring RADIUS authorization

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

  For TACACS+ authorization without authentication, perform the task in Configuring TACACS+ authorization for each participating 7705 SAR router:
- TACACS+ authorization

For TACACS+ authorization with authentication, configure these tasks on each participating 7705 SAR router:

- Enabling TACACS+ authentication
- Configuring TACACS+ authorization

3.8.3 Configuring accounting

See the following sections to configure accounting.

- Local accounting is not implemented. For information about configuring accounting policies, see Configuring logging with CLI.
- Configuring RADIUS accounting
- Configuring TACACS+ accounting

3.9 Security configurations

To implement security features, configure the following components:

- management access filters
- CPM (CSM) filters
- profiles
- user access parameters
- password management parameters
- RADIUS or TACACS+
  - enable one to five RADIUS or TACACS+ (or both) servers
  - configure RADIUS or TACACS+ (or both) parameters

The following example displays default values for security parameters.

```
NOK-1>config>system>security# info detail
----------------------------------------------
            no hash-control
            telnet-server
            no telnet6-server
            ftp-server
            management-access-filter
                ip-filter
                    no shutdown
                exit
                ipv6-filter
                    no shutdown
                exit
            exit
            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 "administrative"
                default-action permit-all
                entry 10
                    no description
                    match "configure system security"
                    action permit
                exit
                entry 20
                    no description
                    match "show system security"
                    action permit
                exit
                entry 30
                    no description
                    match "tools perform security"
                    action permit
                exit
                entry 50
                    no description
                    match "admin system security"
                    action permit
                exit
            exit
            password
                authentication-order radius tacplus local
                no aging
                attempts 3 time 5 lockout 10
```

```
                health-check interval 30
                no admin-password
                hashing bcrypt
                history-size 0
                minimum-age min 10
                minimum-change 5
                complexity-rules
                    no allow-user-name
                    credits lowercase 0 uppercase 0 numeric 0 special-character 0
                    no minimum-classes
                    minimum-length 6
                    no repeated-characters
                    required lowercase 0 uppercase 0 numeric 0 special-character 0
                exit
            exit
            tech-support
                no ts-location
            exit
            user-template "radius_default"
                access console
                profile "default"
                no home-directory
                restricted-to-home
                save-when-restricted
                console
                    no login-exec
                exit
            exit
            user-template "tacplus_default"
                access console
                profile "default"
                no home-directory
                restricted-to-home
                save-when-restricted
                console
                    no login-exec
                exit
            exit
            user "admin"
                password "$2y$10$TQrZlpBDra86.qoexZUzQeBXDY1FcdDhGWdD9lLxMuFyPVSm0OGy6"
                access console
                no home-directory
                no restricted-to-home
                save-when-restricted
                public-keys
                    ecdsa
                    exit
                    rsa
                    exit
                exit
                console
                    no login-exec
                    no cannot-change-password
                    no new-password-at-login
                    member "administrative"
                    local-lockout
                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-mgmt" security-model snmpv1 security-level no-auth-no-
privacy context "management" exact read "mgmt-view" write "mgmt-view" notify "mgmt-view"
                access group "snmp-mgmt" security-model snmpv2c security-level no-auth-no-
privacy context "management" exact read "mgmt-view" write "mgmt-view" notify "mgmt-view"
                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 "snmp-vprn" security-model snmpv1 security-level no-auth-no-
privacy context "vprn" prefix read "vprn-view" write "vprn-view" notify "vprn-view"
                access group "snmp-vprn" security-model snmpv2c security-level no-auth-no-
privacy context "vprn" prefix read "vprn-view" write "vprn-view" notify "vprn-view"
                access group "cli-readonly" security-model snmpv2c security-level no-auth-no-
privacy read "iso" notify "iso"
                access group "snmp-vprn-ro" security-model snmpv1 security-level no-auth-no-
privacy context "vprn" prefix read "vprn-view" notify "vprn-view"
                access group "snmp-vprn-ro" security-model snmpv2c security-level no-auth-no-
privacy context "vprn" prefix read "vprn-view" notify "vprn-view"
                access group "cli-readwrite" security-model snmpv2c security-level no-auth-no-
privacy read "iso" write "iso" notify "iso"
                access group "snmp-vpls-mgmt" security-model snmpv1 security-level no-auth-no-
privacy context "vpls-management" prefix read "mgmt-view" write "mgmt-view" notify "mgmt-view"
                access group "snmp-vpls-mgmt" security-model snmpv2c security-level no-auth-no-
privacy context "vpls-management" prefix read "mgmt-view" write "mgmt-view" notify "mgmt-view"
                access group "cli-vprn-readwrite" security-model snmpv2c security-level no-
auth-no-privacy context "vprn" exact read "vprn-view" write "vprn-view" notify "iso"
                attempts 20 time 5 lockout 10
                community "cV3ISTw2V5pbEWmVEA9jXgB/1EERXQA=" hash2 rwa version both
                community "76HzdddhlPpRo1Vql+ZB5spLqccgYQ==" hash2 r version both
            exit
            ssh
                client-cipher-list
                    cipher 2 name aes256-ctr
                    cipher 4 name aes192-ctr
                    cipher 6 name aes128-ctr
                    cipher 10 name aes128-cbc
                    cipher 20 name 3des-cbc
                    cipher 60 name aes192-cbc
                    cipher 70 name aes256-cbc
                exit
                server-cipher-list
                    cipher 2 name aes256-ctr
                    cipher 4 name aes192-ctr
                    cipher 6 name aes128-ctr
                    cipher 10 name aes128-cbc
                    cipher 20 name 3des-cbc
                    cipher 60 name aes192-cbc
                    cipher 70 name aes256-cbc
                exit
                client-mac-list
                    mac 200 name hmac-sha2-512
                    mac 210 name hmac-sha2-256
```

```
                    mac 215 name hmac-sha1
                    mac 220 name hmac-sha1-96
                    mac 225 name hmac-md5
                    mac 240 name hmac-md5-96
                exit
                server-mac-list
                    mac 200 name hmac-sha2-512
                    mac 210 name hmac-sha2-256
                    mac 215 name hmac-sha1
                    mac 220 name hmac-sha1-96
                    mac 225 name hmac-md5
                    mac 240 name hmac-md5-96
                exit
                client-kex-list
                    kex 200 name diffie-hellman-group16-sha512
                    kex 210 name diffie-hellman-group14-sha256
                    kex 215 name diffie-hellman-group14-sha1
                    kex 220 name diffie-hellman-group-exchange-sha1
                    kex 225 name diffie-hellman-group1-sha1
                exit
                server-kex-list
                    kex 200 name diffie-hellman-group16-sha512
                    kex 210 name diffie-hellman-group14-sha256
                    kex 215 name diffie-hellman-group14-sha1
                    kex 220 name diffie-hellman-group-exchange-sha1
                    kex 225 name diffie-hellman-group1-sha1
                exit
                key-re-exchange
                    client
                        mbytes 1024
                        minutes 60
                        no shutdown
                    exit
                    server
                        mbytes 1024
                        minutes 60
                        no shutdown
                    exit
                exit
                no preserve-key
                no server-shutdown
            exit
            dot1x
                shutdown
            exit
            no vprn-network-exceptions
            cli-script
                authorization
                    cron
                        no cli-user
                    exit
                    event-handler
                        no cli-user
                    exit
                exit
            exit
            cpm-filter
                default-action accept
                ip-filter
                    shutdown
                exit
                ipv6-filter
                    shutdown
                exit
```

```
            exit
            tls
            exit
```

3.10 Security configuration procedures

- Configuring IPv4 or IPv6 management access filters
- Configuring IPv4 or IPv6 CPM (CSM) filters
- Configuring password management parameters
- Managing IPSec certificates
- Configuring profiles
- Configuring users
- Copying and overwriting users and profiles
- Configuring SSH
- Configuring SSH cipher lists
- Configuring SSH KEX algorithm lists
- Configuring SSH MAC algorithm lists
- Configuring login controls
- Configuring RADIUS parameters
- Configuring TACACS+ parameters
- Configuring keychain authentication
- Configuring keychains

3.10.1 Configuring IPv4 or IPv6 management access filters

Creating and implementing management access filters is optional. Management access filters control all traffic going in to the CSM, including all routing protocols. They apply to packets from all ports. The filters can be used to restrict management of the 7705 SAR 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.

Management access filters apply to the management Ethernet port, which supports both IPv4 and IPv6 filters.

The 7705 SAR exits the filter when the first match is found and executes 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 **action** to be considered complete. Entries without the **action** keyword are considered incomplete and are rendered inactive.

Use the following CLI commands to configure an IPv4 management access filter.

CLI syntax:

```
config>system
    security
```

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

Use the following CLI commands to configure an IPv6 management access filter.

CLI syntax:

```
config>system
    security
        management-access-filter
            ipv6-filter
                default-action {permit | deny | deny-host-unreachable}
                entry entry-id
                    action {permit | deny | deny-host-unreachable}
                    description description-string
                    dst-port port [mask]
                    flow-label value
                    log
                    next-header next-header
                    router router-instance
                    src-ip {ipv6-address/prefix-length | ipv6-prefix-
list ipv6-prefix-list-name}
                    src-port {port-id | cpm}
                renum old-entry-number new-entry-number
                no shutdown
```

The following example displays an IPv4 management access filter configuration. This example only accepts packets matching the criteria specified in entries 1 and 2. Non-matching packets are denied.

Example:

```
config>system>security# management-access-filter
config>system>security>mgmt-access-filter# ip-filter default-action
 deny
config>system>security>mgmt-access-filter# ip-filter entry 1
config>system>security>mgmt-access-filter>ip-filter>entry# src-
ip 10.10.10.104/32
config>system>security>mgmt-access-filter>ip-filter>entry# action
 permit
config>system>security>mgmt-access-filter>ip-filter>entry# exit
config>system>security>mgmt-access-filter# entry 2
config>system>security>mgmt-access-filter>ip-filter>entry# src-
ip 10.10.10.1/32
config>system>security>mgmt-access-filter>ip-filter>entry# action
 permit
config>system>security>mgmt-access-filter>ip-filter>entry# exit
```

The following example displays the management access filter configuration.

```
ALU-1>config>system>security# info
```

```
------------------------------------------
            management-access-filter
                ip-filter
                default-action deny
                entry 1
                    action permit
                    src-ip 10.10.10.104/32
                exit
                entry 2
                    action permit
                    src-ip 10.10.0.1/32
                exit
            exit
------------------------------------------
ALU-1>config>system>security#
```

Note: If configuring management access filters via a Telnet session, ensure that data from the host IP address is permitted before setting the default action to **deny**; otherwise, the session is dropped. To do this, set the default action to **permit**, configure an entry with the **src-ip** address of the host as a permitted match criterion, then set the default action back to **deny**. Alternatively, use a direct console connection to the node for configuration; in this case, the order of filter configuration does not matter.

3.10.2 Configuring IPv4 or IPv6 CPM (CSM) filters

CPM filters control all traffic going in to the CSM, including all routing protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port. CPM packet filtering is performed by network processor hardware using no resources on the main CPUs.

Use the following CLI commands to configure an IPv4 CPM filter.

CLI syntax:

```
config>system>security
cpm-filter
    default-action {accept | drop}
    ip-filter
        entry entry-id [create]
            action {accept | drop}
            description description-string
            log log-id
            match [protocol protocol-id]
                dscp dscp-name
                dst-ip {ip-address/mask | ip-address ipv4-address-mask
 | ip-prefix-list prefix-list-name}
                dst-port [tcp/udp port-number] [mask]
                fragment {true | false}
                icmp-code icmp-code
                icmp-type icmp-type
                ip-option ip-option-value [ip-option-mask]
                multiple-option {true | false}
                option-present {true | false}
                src-ip {ip-address/mask | ip-address ipv4-address-mask
 | ip-prefix-list prefix-list-name}
                src-port src-port-number [mask]
                tcp-ack {true | false}
                tcp-syn {true | false}
            renum old-entry-id new-entry-id
```

Use the following CLI commands to configure an IPv6 CPM filter.

CLI syntax:

```
config>system>security
cpm-filter
    default-action {accept | drop}
    ipv6-filter
        entry entry-id [create]
            action {accept | drop}
            description description-string
            log log-id
            match [next-header next-header]
            dscp dscp-name
            dst-ip {ipv6-address/prefix-length | ipv6-prefix-list
 ipv6-prefix-list-name}
            dst-port [tcp/udp port-number] [mask]
            icmp-code icmp-code
            icmp-type icmp-type
            src-ip {ipv6-address/prefix-length | ipv6-prefix-
list ipv6-prefix-list-name}
            src-port src-port-number [mask]
            tcp-ack {true | false}
            tcp-syn {true | false}
            renum old-entry-id new-entry-id
```

The following displays an IPv4 CPM filter configuration example:

```
A:ALU-49>config>sys>sec>cpm>ip-filter# info
----------------------------------------------
                    entry 10 create
                        action drop
                        description "CPM-Filter 10.4.101.2 #101"
                        log 101
                    exit
                    entry 20 create
                        no action
                        description "CPM-Filter 10.4.101.2 #201"
                        log 101
                    exit
                    no shutdown
----------------------------------------------
A:ALU-49>config>sys>sec>cpm>ip-filter#
```

3.10.3 Configuring password management parameters

Depending on the authentication requirements, password parameters are configured locally or on the RADIUS or TACACS+ server.

Use the following CLI commands to configure password support:

CLI syntax:

```
config>system>security
    password
        admin-password password [hash | hash2]
        aging days
        attempts count [time minutes1] [lockout minutes2]
        authentication-order [method-1] [method-2] [method-3] [exit-
on-reject]
        complexity-rules
        hashing hashing {bcrypt | sha2-pbkdf2 | sha3-pbkdf2}
```

```
        health-check [interval interval]
        history-size size
        minimum-age [days days] [hrs hours][min minutes] [sec seconds]
        minimum-change distance
```

The following example displays the default password configuration:

```
*A:Dut-A>config>system>security>password# info detail
----------------------------------------------
               authentication-order radius tacplus local
               no aging
               attempts 3 time 5 lockout 10
               health-check interval 30
               no admin-password
               hashing bcrypt
               history-size 0
               minimum-age min 10
               minimum-change 5
               complexity-rules
                   no allow-user-name
                   credits lowercase 0 uppercase 0 numeric 0 special-character 0
                   no disallow-sequence-keys
                   no minimum-classes
                   minimum-length 6
                   no repeated-characters
                   required lowercase 0 uppercase 0 numeric 0 special-character 0
               exit
----------------------------------------------
```

3.10.4 Managing IPSec certificates

The following is an example of importing a certificate from a **pem** format:

```
*A:ALU-A# admin certificate import type cert input cf3:/pre-import/
R10cert.pem output R1-0cert.der format pem
```

The following is an example of exporting a certificate to a **pem** format:

```
*A:ALU-A#  admin certificate export type cert input R1-0cert.der output cf3:/
R10cert.pem format pem
```

The following example displays a profile output:

```
*A:ALU-A>config>system>security>pki# info
----------------------------------------------
            ca-profile "Root" create
                description "Root CA"
                cert-file "R1-0cert.der"
                crl-file "R1-0crl.der"
                no shutdown
            exit
----------------------------------------------
*A:ALU-A>config>system>security>pki#
```

The following example displays an **ike-policy** with **cert-auth** output:

```
*A:ALU-A>config>ipsec>ike-policy# info
```

```
-----------------------------------------
            auth-method cert-auth
            own-auth-method psk
-----------------------------------------
```

The following example displays a static LAN-to-LAN configuration using **cert-auth**:

```
         interface "VPRN1" tunnel create
             sap tunnel-1.private:1 create
                  ipsec-tunnel "Sanity-1" create
                      security-policy 1
                      local-gateway-address 192.168.0.0 peer 192.168.0.1 delivery-
                       service 300
                      dynamic-keying
                         ike-policy 1
                         pre-shared-key "Sanity-1"
                         transform 1
                         cert
                           trust-anchor-profile "trustAnchorProfile_1"
                           cert-profile "certProfile_4"
                       exit
                    exit
                  no shutdown
              exit
```

3.10.5 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 16 user profiles can be defined. A user can participate in up to 16 profiles. Depending on the authorization requirements, passwords are configured locally or on the RADIUS server.

When configuring profiles, put more specific commands in the lower-numbered entries because the lower-numbered entries take precedence over the higher-numbered entries.

In the following example, because the general command in entry 10 takes precedence, entry 20 is ignored and the "show system" command will be permitted because it matches on "show". To avoid this, the "show system" entry needs to be a number lower than 10.

Example:

```
entry 10
    match "show"
    action permit
exit
entry 20
    match "show system"
    action deny
exit
```

Note: security commands in the **config>system**, **show>system**, **admin>system**, and **tools>perform** contexts that are not explicitly permitted are automatically denied.

Use the following CLI commands to configure user profiles:

CLI syntax:

```
config>system>security
    profile user-profile-name
    default-action {deny-all | permit-all | none}
```

```
    renum old-entry-number new-entry-number
    entry entry-id
        description description-string
        match command-string
        action {permit | deny}
```

The following displays an example of the user profile command usage.

Example:

```
config>system>security# profile ghost
config>system>security>profile$ default-action permit-all
config>system>security>profile# entry 1
config>system>security>profile>entry$ action permit
config>system>security>profile>entry# match "configure"
config>system>security>profile>entry# exit
config>system>security>profile# entry 2
config>system>security>profile>entry$ match "show"
config>system>security>profile>entry# exit
config>system>security>profile# entry 3
config>system>security>profile>entry$ match "exit"
```

The following example displays the user profile output:

```
ALU-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
```

3.10.6 Configuring users

Access parameters are configured for individual users. For each user, the login name and, optionally, information that identifies the user is defined. Use the following CLI syntax to configure access parameters for users. The **snmp authentication des-key** keyword is not available if the 7705 SAR node is running in FIPS-140-2 mode.

CLI syntax:

```
config>system>security
    user user-name
        access [ftp] [snmp] [console] [scp-sftp] [console-port-cli]
 [ssh-cli] [telnet-cli]
        console
            cannot-change-password
            local-lockout
            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]
        restricted-to-home
        save-when-restricted
        snmp
            authentication {[none] | [[hash] {md5 key-1 | sha key-1}
privacy {none | des-key key-2 | aes-128-cfb-key key-2}]}
            group group-name
```

The following example displays the user configuration, including default values:

```
NOK-1>config>system>security# info detail
----------------------------------------------
...
        user "test"
                password "$2y$10$NXW9rLCSdBZiSUZ0fQGI2.mLh4ofLpXKAnay5SPSDVQI5FtKCottq"
                access console
                no home-directory
                restricted-to-home
                save-when-restricted
                public-keys
                    ecdsa
                    exit
                    rsa
                    exit
                exit
                console
                    no login-exec
                    no cannot-change-password
                    no new-password-at-login
                    member "default"
                    local-lockout
                exit
            exit
            snmp
                view "iso" subtree "1"
                    mask ff type included
                exit
...
----------------------------------------------
NOK-1>config>system>security#
```

Note: The **restricted-to-home** default setting applies to non-administrative users. For administrative users (**user "admin"**), the default is **no restricted-to-home** as shown in Security configurations.

3.10.7 Copying and overwriting users and profiles

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

3.10.7.1 Copying a user

CLI syntax:

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

Example:

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

The following output displays the copied user configurations:

```
ALU-12>config>system>security# info
----------------------------------------------
...
            user "testuser"
                password "$2y$10$siOU8NvWRzFFtJjO5wA1I.7mr.57emDXUC14p6EZtO.pmr0aqL
Sa"
                access snmp
                snmp
                    authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy
 none
                    group "testgroup"
                exit
            exit
            user "testuserA"
                password "$2y$10$siOU8NvWRzFFtJjO5wA1I.7mr.57emDXUC14p6EZtO.pmr0aqLW
Sa"
                access snmp
                console
                    new-password-at-login
                exit
                snmp
                    authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy
 none
                    group "testgroup"
                exit
            exit
...
----------------------------------------------
ALU-12>config>system>security# info
```

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

```
ALU-12>config>system>security>user# info
----------------------------------------------
    password "$2y$10$siOU8NvWRzFFtJjO5wA1I.7mr.57emDXUC14p6EZtO.pmr0aqLWSa"
    access snmp
    console
        cannot-change-password
    exit
    snmp
        authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
```

```
        group "testgroup"
    exit
-----------------------------------------------
ALU-12>config>system>security>user# exit
ALU-12>config>system>security# user testuserA
ALU-12>config>system>security>user# info
-----------------------------------------------
    password "$2y$10$siOU8NvWRzFFtJjO5wA1I.7mr.57emDXUC14p6EZtO.pmr0aqLWSa"
    access snmp
    console
        new-password-at-login
    exit
    snmp
        authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
        group "testgroup"
    exit
-----------------------------------------------
ALU-12>config>system>security>user#
```

3.10.7.2 Copying a profile

CLI syntax:

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

Example:

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

The following output displays the copied profiles:

```
A:ALU-49>config>system>security# info
-----------------------------------------------
...
A:ALU-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
...
```

3.10.8 Configuring SSH

Use the **ssh** command to configure the SSH server. This command should only be enabled or disabled when the SSH server is disabled. This setting cannot be changed while the SSH server is running.

CLI syntax:

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

Example:

```
config>system>security# ssh
config>system>security>ssh# preserve-key
```

The following example displays the SSH server configuration using a host-key:

```
A:ALU-1>config>system>security>ssh# info
----------------------------------------------
                preserve-key
----------------------------------------------
A:ALU-1>config>system>security>ssh#
```

3.10.9 Configuring SSH cipher lists

Use the **ssh** command to configure SSHv2 cipher lists. Client cipher lists are used if the 7705 SAR is acting as an SSH client, and server cipher lists are used if the 7705 SAR is acting as an SSH server.

Note: When the 7705 SAR is running in FIPS-140-2 mode, the 3des-cbc cipher is not available.

CLI syntax:

```
config>system>security
    ssh
        client-cipher-list
            cipher index name cipher-name
        server-cipher-list
            cipher index name cipher-name
```

Example:

```
config>system>security# ssh
config>system>security>ssh# client-cipher-list
config>system>security>ssh>client-cipher# cipher 2 name aes256-ctr
config>system>security>ssh>client-cipher# cipher 4 name aes128-ctr
config>system>security>ssh>client-cipher# cipher 6 name aes256-cbc
config>system>security>ssh>client-cipher# cipher 10 name aes128-cbc
config>system>security>ssh>client-cipher# cipher 20 name 3des-cbc
config>system>security>ssh>client-cipher# cipher 60 name aes192-cbc
config>system>security>ssh>client-cipher# cipher 70 name aes256-cbc
config>system>security>ssh>client-cipher# exit
config>system>security>ssh# server-cipher-list
```

```
config>system>security>ssh>server-cipher# cipher 2 name aes256-ctr
config>system>security>ssh>server-cipher# cipher 4 name aes192-ctr
config>system>security>ssh>server-cipher# cipher 6 name aes128-ctr
config>system>security>ssh>server-cipher# cipher 10 name aes128-cbc
config>system>security>ssh>server-cipher# cipher 20 name 3des-cbc
config>system>security>ssh>server-cipher# cipher 60 name aes192-cbc
config>system>security>ssh>server-cipher# cipher 70 name aes256-cbc
config>system>security>ssh>server-cipher# exit
config>system>security>ssh# exit
```

The following example displays SSHv2 client and server cipher list configurations:

```
A:Sar8 Dut-A>config>system>security>ssh# info detail
----------------------------------------------
                client-cipher-list
                    cipher 2 name aes256-ctr
                    cipher 4 name aes192-ctr
                    cipher 6 name aes128-ctr
                    cipher 10 name aes128-cbc
                    cipher 20 name 3des-cbc
                    cipher 60 name aes192-cbc
                    cipher 70 name aes256-cbc
                exit
                server-cipher-list
                    cipher 2 name aes256-ctr
                    cipher 4 name aes192-ctr
                    cipher 6 name aes128-ctr
                    cipher 10 name aes128-cbc
                    cipher 20 name 3des-cbc
                    cipher 60 name aes192-cbc
                    cipher 70 name aes256-cbc
                exit
----------------------------------------------
*A:Sar8 Dut-A>config>system>security>ssh#
```

3.10.10 Configuring SSH KEX algorithm lists

Use the **ssh** command to configure SSHv2 client and server KEX algorithm lists. Client KEX algorithm lists are used if the 7705 SAR is acting as an SSH client, and server KEX algorithm lists are used if the 7705 SAR is acting as an SSH server.

Note: When the 7705 SAR node is running in FIPS-140-2 mode, the diffie-hellman-group1-sha1 KEX algorithm is not available.

CLI syntax:

```
config>system>security
    ssh
        client-kex-list
            kex index name kex-name
        server-kex-list
            kex index name kex-name
```

Example:

```
config>system>security# ssh
config>system>security>ssh# client-kex-list
config>system>security>ssh>client-kex# kex 200 name diffie-hellman-
group16-sha512
```

```
config>system>security>ssh>client-kex# kex 210 name diffie-hellman-
group14-sha256
config>system>security>ssh>client-kex# kex 215 name diffie-hellman-
group14-sha1
config>system>security>ssh>client-kex# kex 220 name diffie-hellman-
group-exchange-sha1
config>system>security>ssh>client-kex# kex 225 name diffie-hellman-
group1-sha1
config>system>security>ssh>client-kex# exit
config>system>security>ssh# server-kex-list
config>system>security>ssh>server-kex# kex 200 name diffie-hellman-
group16-sha512
config>system>security>ssh>server-kex# kex 210 name diffie-hellman-
group14-sha256
config>system>security>ssh>server-kex# exit
config>system>security>ssh# exit
```

The following example displays SSHv2 client and server KEX list configurations:

```
A:Sar8 Dut-A>config>system>security>ssh# info detail
----------------------------------------------
                client-kex-list
                    kex 200 name diffie-hellman-group16-sha512
                    kex 210 name diffie-hellman-group14-sha256
                    kex 215 name diffie-hellman-group14-sha1
                    kex 220 name diffie-hellman-group-exchange-sha1
                    kex 225 name diffie-hellman-group1-sha1
                exit
                server-kex-list
                    kex 200 name diffie-hellman-group16-sha512
                    kex 210 name diffie-hellman-group14-sha256
                    kex 215 name diffie-hellman-group14-sha1
                    kex 220 name diffie-hellman-group-exchange-sha1
                    kex 225 name diffie-hellman-group1-sha1
                exit
----------------------------------------------
*A:Sar8 Dut-A>config>system>security>ssh#
```

3.10.11 Configuring SSH MAC algorithm lists

Use the **ssh** command to configure SSHv2 client and server MAC algorithm lists. Client MAC algorithm lists are used if the 7705 SAR is acting as an SSH client, and server MAC algorithm lists are used if the 7705 SAR is acting as an SSH server.

Note: When the 7705 SAR node is running in FIPS-140-2 mode, the following MAC algorithms are not available:

- hmac-sha1-96
- hmac-md5
- hmac-mda5-96

CLI syntax:

```
config>system>security
    ssh
        client-mac-list
            mac index name mac-name
        server-mac-list
```

```
            mac index name mac-name
```

Example:

```
config>system>security# ssh
config>system>security>ssh# client-mac-list
config>system>security>ssh>client-mac# mac 200 name hmac-sha2-512
config>system>security>ssh>client-mac# mac 210 name hmac-sha2-256
config>system>security>ssh>client-mac# mac 215 name hmac-sha1
config>system>security>ssh>client-mac# mac 220 name hmac-sha1-96
config>system>security>ssh>client-mac# mac 225 name hmac-md5
config>system>security>ssh>client-mac# mac 240 name hmac-md5-96
config>system>security>ssh>client-mac# exit
config>system>security>ssh# server-mac-list
config>system>security>ssh>server-mac# mac 200 name hmac-sha2-512
config>system>security>ssh>server-mac# mac 210 name hmac-sha2-256
config>system>security>ssh>server-mac# exit
config>system>security>ssh# exit
```

The following example displays client and server MAC list configurations:

```
A:Sar8 Dut-A>config>system>security>ssh# info detail
----------------------------------------------
                client-mac-list
                    mac 200 name hmac-sha2-512
                    mac 210 name hmac-sha2-256
                    mac 215 name hmac-sha1
                    mac 220 name hmac-sha1-96
                    mac 225 name hmac-md5
                    mac 240 name hmac-md5-96
                exit
                server-mac-list
                    mac 200 name hmac-sha2-512
                    mac 210 name hmac-sha2-256
                    mac 215 name hmac-sha1
                    mac 220 name hmac-sha1-96
                    mac 225 name hmac-md5
                    mac 240 name hmac-md5-96
                exit
                exit
----------------------------------------------
*A:Sar8 Dut-A>config>system>security>ssh#
```

3.10.12 Configuring login controls

Use the **login-control** context to configure parameters for console, FTP, SSH, and Telnet sessions.

CLI syntax:

```
config>system
    login-control
        exponential-backoff
        ftp
            inbound-max-sessions value
        ssh
            [no] disable-graceful-shutdown
            inbound-max-sessions value
            outbound-max-sessions value
            ttl-security min-ttl-value
        telnet
            [no] enable-graceful-shutdown
```

```
            inbound-max-sessions value
            outbound-max-sessions value
            ttl-security min-ttl-value
        idle-timeout {minutes | disable}
        pre-login-message login-text-string [name]
        login-banner
        motd {url url-prefix:source-url | text motd-text-string}
```

The following example displays the login control configuration:

Example:

```
config>system>login-control# ftp inbound-max-sessions 5
config>system>login-control# ssh inbound-max-sessions 12
config>system>login-control# ssh outbound-max-sessions 8
config>system>login-control# ssh ttl-security 100
config>system>login-control# telnet enable-graceful-shutdown
config>system>login-control# telnet inbound-max-sessions 7
config>system>login-control# telnet outbound-max-sessions 2
config>system>login-control# idle-timeout 1440
config>system>login-control# pre-login-message "Property of Service
 Routing Inc. Unauthorized access prohibited."
config>system>login-control# motd text "Notice to all users: Software
 upgrade scheduled 3/2 1:00 AM"
```

The following example displays the login control configuration:

```
ALU-1>config>system# info
----------------------------------------------
...
       login-control
           ftp
               inbound-max-sessions 5
           exit
           ssh
               no disable-graceful-shutdown
               inbound-max-sessions 12
               outbound-max-sessions 8
               ttl-security  100
           telnet
               enable-graceful-shutdown
               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
...
----------------------------------------------
ALU-1>config>system#
```

3.10.13 Configuring RADIUS parameters

- Configuring RADIUS authentication
- Configuring RADIUS authorization
- Configuring RADIUS accounting

- Configuring 802.1x RADIUS policies

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

Also, the system IP address must be configured in order for the RADIUS client to work. See "Configuring a System Interface" in the 7705 SAR Router Configuration Guide.

The other commands are optional.

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

CLI syntax:

```
config>system>security
    radius
        port port
        retry count
        server server-index address ip-address secret key [hash1 |
 hash2]
        timeout seconds
        no shutdown
```

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
security# radius
security# no shutdown
security>radius# server 1 address A:A:A:A:A:A:A:1 secret test11
security>radius# server 2 address 10.10.0.1 secret test2
security>radius# server 3 address 10.10.0.2 secret test3
security>radius# server 4 address 10.10.0.3 secret test4
security>radius# retry 5
security>radius# timeout 5
config>system>security>radius# exit
```

The following example displays the RADIUS authentication configuration:

```
ALU-1>config>system>security# info
----------------------------------------------
                retry 5
                timeout 5
                server 1 address A:A:A:A:A:A:A:1 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"
...
----------------------------------------
ALU-1>config>system>security#
```

3.10.13.2 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 RADIUS VSAs.

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

CLI syntax:

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

The following example displays the CLI syntax usage:

Example:

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

The following example displays the RADIUS authorization configuration:

```
ALU-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
...
----------------------------------------------
```

3.10.13.3 Configuring RADIUS accounting

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

CLI syntax:

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

The following example displays the CLI syntax usage:

Example:

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

The following example displays the RADIUS accounting configuration:

```
ALU-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
...
----------------------------------------------
ALU-1>config>system>security#
```

3.10.13.4 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 on Ethernet ports. See the 7705 SAR Interface Configuration Guide, "Configuration Command Reference", for more information about configuring 802.1x parameters on Ethernet ports.

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

CLI syntax:

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

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
config>system>security# dot1x
config>system>security>dot1x# radius-plcy dot1x_plcy
create
config>system>security>dot1x>radius-plcy# server 1 address 10.10.10.1
 secret abc auth-port 65000
config>system>security>dot1x>radius-plcy# server 2 address 10.10.10.3
 secret xyz auth-port 862
config>system>security>dot1x>radius-plcy# source-address 10.10.10.255
```

The following example displays an 802.1x configuration:

```
*A:7705_custDoc>config>system>security>dot1x# info
----------------------------------------------
```

```
        radius-plcy "dot1x_plcy" create
            server 1 address 10.10.10.1 auth-port 65000 acct-
port 1813 secret "WDoQz6DJf4.0M5dlpwjHbk" hash2 type authorization
            server 2 address 10.10.10.3 auth-port 862 acct-port 1813 secret
 "WDoQz6DJf4.j1WcCeHZwz." hash2 type authorization
            source-address 10.10.10.255
            shutdown
        exit
...
-----------------------------------------------
A:ALU-1>config>system#
```

3.10.14 Configuring TACACS+ parameters

- Enabling TACACS+ authentication
- Configuring TACACS+ authorization
- Configuring TACACS+ accounting

3.10.14.1 Enabling TACACS+ authentication

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

Use the following CLI commands to configure TACACS+ authentication:

CLI syntax:

```
config>system>security
    tacplus
        server server-index address ip-address secret key [hash1 |
 hash2]
        timeout seconds
        no shutdown
```

The following example is configured in the **config>system** context:

Example:

```
security# tacplus
security>tacplus# server 1 address A:A:A:A:A:A:A:1 secret test1
security>tacplus# server 2 address 10.10.0.6 secret test2
security>tacplus# server 3 address 10.10.0.7 secret test3
security>tacplus# server 4 address 10.10.0.8 secret test4
security>tacplus# server 5 address 10.10.0.9 secret test5
config>system>security>tacplus# timeout 5
config>system>security>tacplus# no shutdown
```

The following example displays the TACACS+ authentication configuration:

```
ALU-1>config>system>security>tacplus# info
-----------------------------------------------
               timeout 5
               server 1 address A:A:A:A:A:A:A:1 secret "h6.TeL7YPohbmhlvz0gob."
          hash2
               server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
               server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
               server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
               server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
```

3.10.14.2 Configuring TACACS+ authorization

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

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

CLI syntax:

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

The following example displays the CLI syntax usage:

Example:

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

The following example displays the TACACS+ authorization configuration:

```
ALU-1>config>system>security>tacplus# info
----------------------------------------------
                authorization
                timeout 5
                server 1 address 10.10.0.5 secret "h6.TeL7YPohbmhlvz0gob." hash2
                server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
                server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
                server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
                server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
----------------------------------------------
ALU-1>config>system>security>tacplus#
```

3.10.14.3 Configuring TACACS+ accounting

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

CLI syntax:

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

The following example displays the CLI syntax usage:

Example:

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

The following example displays the TACACS+ accounting configuration:

```
ALU-1>config>system>security>tacplus# info
----------------------------------------------
                accounting
```

```
                authorization
                timeout 5
                server 1 address 10.10.0.5 secret "h6.TeL7YPohbmhlvz0gob." hash2
                server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
                server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
                server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
                server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
------------------------------------------------
ALU-1>config>system>security>tacplus#
```

3.10.15 Configuring keychain authentication

The keychain authentication mechanism protects communication between routing protocol neighbors against malicious attacks. Keychain authentication provides the ability to configure authentication keys and update them through key rollover without affecting the state of the routing protocol adjacencies. See Key rollover for more information about **begin-time** and **end-time** configuration.

This procedure describes how to set up keychain authentication.

Note: The user must perform this procedure on both devices that will use keychain authentication to communicate.

Procedure

Step 1. Configure the keychain instance using the following command:

Note: A keychain must be configured on the system before it can be applied to a session.

```
config>system>security>keychain name
```

Step 2. Configure keychain authentication under the **keychain** context. The keychain must have at least one valid entry and an authentication algorithm:

```
config>system>security>keychain
            direction
                bi
                    entry entry-id [key authentication-key | hash-key | hash2-key
 [hash | hash2] algorithm algorithm]
                        begin-time [date] [hours-minutes] [UTC]
                    exit
                    entry entry-id2 [key authentication-key | hash-key | hash2-key
 [hash | hash2] algorithm algorithm]
                        begin-time [date] [hours-minutes] [UTC]
                    exit
                exit
            exit
            no shutdown
```

Step 3. Associate the configured authentication keychain with a protocol; for example:

```
config>router# isis [isis-instance]
    auth-keychain name
    level {1 | 2}
        auth-keychain name
```

Depending on the protocol, authentication keychains can be used for authentication at the global, level, and interface contexts. For IS-IS, Hello authentication keychains can be used for authentication at the interface and interface level contexts.

3.10.16 Configuring keychains

The keychain mechanism allows for the creation of keys used to authenticate protocol communications. Each keychain entry defines the authentication attributes to be used in authenticating protocol messages from remote peers or neighbors; the keychain must include at least one key entry to be valid.

Each key within a keychain must include the following attributes for the authentication of protocol messages:

- key identifier
- authentication algorithm
- authentication key
- direction
- begin time

Optionally, each key can include an end time and tolerance.

Use the following CLI commands to configure a keychain:

CLI syntax:

```
config>system>security
    keychain name
        description description-string
        direction
            bi
                entry entry-id [key authentication-key | hash-
key | hash2-key [hash | hash2] algorithm algorithm]
                    begin-time [date] [hours-minutes] [UTC]
                    tolerance {seconds | forever}
            uni
                receive
                    entry entry-id [key authentication-key | hash-
key | hash2-key [hash | hash2] algorithm algorithm]
                        begin-time [date] [hours-minutes] [UTC]
                        tolerance {seconds | forever}
            send
                entry entry-id [key authentication-key | hash-
key | hash2-key [hash | hash2] algorithm algorithm]
                    begin-time [date] [hours-minutes] [UTC]
```

The following example displays a keychain configuration:

```
A:ALU-1>config>system>security># info detail
----------------------------------------------
...
            keychain "ospf-md5"
                description "MD5 keychain for OSPF interfaces"
                tcp-option-number
                    send 254
                    receive 254
                exit
                direction
```

```
                    bi
                        entry 0 key "VyScMGuUfEQw9vxb9YWEG8oEeyRxTrGC.aFwWKzlO1E
" hash2 algorithm message-digest
                            no shutdown
                            begin-time 2016/06/01 00:00:00 UTC
                            no option
                        exit
                        entry 1 key "VyScMGuUfEQw9vxb9YWEG6rfIEGa/.sGbxt3BaeWYO.
" hash2 algorithm message-digest
                            no shutdown
                            begin-time 2016/06/09 00:00:00 UTC
                            no option
                            tolerance 600
                        exit
                    exit
                exit
                no shutdown
            exit
            keychain "rsvp-md5"
                description "MD5 keychain for RSVP interfaces"
                tcp-option-number
                    send 254
                    receive 254
                exit
                direction
                    uni
                        send
                            entry 0 key "f4L8216viTz8OMIKEcNfF/0BxU12MaZskrUHlTN
YMwY" hash2 algorithm message-digest
                                no shutdown
                                begin-time 2016/06/01 00:00:00 UTC
                            exit
                            entry 1 key "f4L8216viTz8OMIKEcNfF0VmwDJEUYqX1ob50zL
E0HY" hash2 algorithm message-digest
                                no shutdown
                                begin-time 2016/06/09 00:00:00 UTC
                            exit
                        exit
                        receive
                            entry 0 key "dE.xAjca3DLqssbdJ8zc8vblBwYsvFXL57dvJEu
RQHE" hash2 algorithm message-digest
                                no shutdown
                                begin-time 2016/06/01 00:00:00 UTC
                                tolerance 600
                            exit
                            entry 1 key "dE.xAjca3DLqssbdJ8zc4ty4BxUSFV5xl9ejgfr
YHGG" hash2 algorithm message-digest
                                no shutdown
                                begin-time 2016/06/09 00:00:00 UTC
                                tolerance 600
                        exit
                    exit
                exit
-----------------------------------------------
A:ALU-1>config>system>security#
```

In the above example, two separate keychains are created, "ospf-md5" and "rsvp-md5", each with two possible keys.

For ospf-md5:

- entry 0 is valid starting at midnight (UTC) on 2016/06/01
- entry 1 will become valid at midnight (UTC) on 2016/06/09 and will replace entry 0

- there is an overlap (tolerance) period of 600 seconds in which packets with either key (entry 0 or entry 1) will be accepted

For rsvp-md5:

- for transmitted packets:
  - send key entry 0 is valid starting at midnight (UTC) on 2016/06/01
  - send key entry 1 will become valid at midnight (UTC) on 2016/06/09 and will replace entry 0
- for received packets:
  - receive key entry 0 is valid starting at midnight (UTC) on 2016/06/01
  - receive key entry 1 will become valid at midnight (UTC) on 2016/06/09 and will replace entry 0
  - there is an overlap (tolerance) period of 600 seconds in which receive packets with either key (entry 0 or entry 1) will be accepted

3.11 Security command reference

3.11.1 Command hierarchies

- Admin commands
- Configuration commands
  - Security configuration commands
  - Management access filter commands
  - IPv6 management access filter commands
  - CPM filter commands
  - IPv6 CPM filter commands
  - Password commands
  - Profile commands
  - User commands
  - CLI script authorization commands
  - RADIUS commands
  - TACACS+ commands
  - 802.1x commands
  - SSH commands
  - TLS commands
  - Keychain authentication commands
  - Login control commands
- Show commands
  - Security commands
  - Login control commands
- Clear commands
  - Admin commands
  - Authentication commands
- Monitor commands
- Debug commands

3.11.1.1 Admin commands

```
admin
    - system
        - security
            - system-password admin-password
```

3.11.1.2 Configuration commands

3.11.1.2.1 Security configuration commands

```
config
- system
        - security
            - copy {user source-user | profile source-profile} to destination [overwrite]
            - ftp-server
            - no ftp-server
            - hash-control [read-version {1 | 2 | all}] [write-version {1 | 2}]
            - no hash-control
            - source-address
                - application app [ip-int-name | ip-address]
                - no application app
                - application6 app ipv6-address
                - no application6 app
            - telnet
                -listening-port port
                -no listening-port
            - [no] telnet-server
            - [no] telnet6-server
            - vprn-network-exceptions [number seconds]
            - no vprn-network-exceptions
```

3.11.1.2.2 Management access filter commands

```
config
- system
        - security
            - [no] management-access-filter
                - 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
                        - [no] log
                        - [no] protocol  protocol-id
                        - router router-instance
                        - router service-name service-name
                        - no router
                        - src-ip {ip-prefix [/mask] [netmask] | ip-prefix-list ip-prefix-list-
name}
                        - no src-ip
                        - src-port {port-id | cpm | lag lag-id}
                        - no src-port
                    - renum old-entry-number new-entry-number
                    - [no] shutdown
```

3.11.1.2.3 IPv6 management access filter commands

```
config
- system
        - security
            - [no] management-access-filter
                - 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
                        - [no] log
                        - [no] next-header next-header
                        - router router-instance
                        - router service-name service-name
                        - no router
                        - src-ip {ipv6-address/prefix-length | ipv6-prefix-list ipv6-prefix-
list-name}
                        - no src-ip
                        - src-port {port-id | cpm | lag lag-id}
                        - no src-port
                    - renum old-entry-number new-entry-number
                    - [no] shutdown
```

3.11.1.2.4 CPM filter commands

```
config
- system
        - security
            - [no] cpm-filter
                - default-action {accept | drop}
                - ip-filter
                    - entry entry-id [create]
                    - no entry entry-id
                        - action {accept | drop}
                        - no action
                        - description description-string
                        - no description
                        - log log-id
                        - no log
                        - match [protocol protocol-id]
                        - no match
                            - dscp dscp-name
                            - no dscp
                            - dst-ip {ip-address/mask | ip-address ipv4-address-mask | ip-
prefix-list prefix-list-name}
                            - no dst-ip
                            - dst-port tcp/udp port-number [mask]
                            - no dst-port
                            - fragment {true | false}
                            - no fragment
                            - icmp-code icmp-code
                            - no icmp-code
```

```
                            - icmp-type icmp-type
                            - no icmp-type
                            - ip-option ip-option-value [ip-option-mask]
                            - no ip-option
                            - multiple-option {true | false}
                            - no multiple-option
                            - option-present {true | false}
                            - no option-present
                            - src-ip {ip-address/mask | ip-address ipv4-address-mask | ip-
prefix-list prefix-list-name}
                            - no src-ip
                            - src-port tcp/udp port-number [mask]
                            - no src-port
                            - tcp-ack {true | false}
                            - no tcp-ack
                            - tcp-syn {true | false}
                            - no tcp-syn
                        - renum old-entry-id new-entry-id
                        - [no] shutdown
```

3.11.1.2.5 IPv6 CPM filter commands

```
config
- system
        - security
            - [no] cpm-filter
                - default-action {accept | drop}
                - ipv6-filter
                    - entry entry-id [create]
                    - no entry entry-id
                        - action {accept | drop}
                        - no action
                        - description description-string
                        - no description
                        - log log-id
                        - no log
                        - match [next-header next-header]
                        - no match
                            - dscp dscp-name
                            - no dscp
                            - dst-ip {ipv6-address/prefix-length | ipv6-prefix-list ipv6-
prefix-list-name}
                            - no dst-ip
                            - dst-port tcp/udp port-number [mask]
                            - no dst-port
                            - icmp-code icmp-code
                            - no icmp-code
                            - icmp-type icmp-type
                            - no icmp-type
                            - src-ip {ipv6-address/prefix-length | ipv6-prefix-list ipv6-
prefix-list-name}
                            - no src-ip
                            - src-port tcp/udp port-number [mask]
                            - no src-port
                            - tcp-ack {true | false}
                            - no tcp-ack
                            - tcp-syn {true | false}
                            - no tcp-syn
                        - renum old-entry-id new-entry-id
                        - [no] shutdown
```

3.11.1.2.6 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
                    - disallow-sequence-keys value
                    - no disallow-sequence-keys
                    - minimum-classes minimum
                    - no minimum-classes
                    - minimum-length value
                    - no minimum-length
                    - repeated-characters count
                    - no repeated-characters
                    - required [lowercase count] [uppercase count] [numeric count] [special-
character count]
                    - no required
                - hashing hashing {bcrypt | sha2-pbkdf2 | sha3-pbkdf2}
                - [no] health-check [interval interval]
                - history-size size
                - no history-size
                - minimum-age [days days] [hrs hours] [min minutes] [sec seconds]
                - no minimum-age
                - minimum-change length
                - no minimum-change
```

3.11.1.2.7 Profile commands

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

3.11.1.2.8 User commands

```
config
- system
        - security
            - [no] user user-name
                - [no] access [ftp] [snmp] [console] [scp-sftp] [console-port-cli] [ssh-cli]
 [telnet-cli]
                - console
                    - [no] cannot-change-password
                    - [no] local-lockout
                    - login-exec url-prefix:source-url
                    - no login-exec
                    - member user-profile-name [user-profile-name…(up to 8 max)]
                    - no member user-profile-name
                    - [no] new-password-at-login
                - home-directory url-prefix [directory] [directory/directory…]
                - no home-directory
                - password [password]
                - public-keys
                    - ecdsa
                        - [no] ecdsa-key key-id [create]
                            - description description-string
                            - no description
                            - key-value public-key-value
                            - no key-value
                    - rsa
                        - [no] rsa-key key-id [create]
                            - description description-string
                            - no description
                            - key-value public-key-value
                            - no key-value
                - [no] restricted-to-home
                - [no] save-when-restricted
                - snmp
                    - authentication none
                    - authentication authentication-protocol authentication-key [privacy none]
 [hash | hash2]
                    - authentication authentication-protocol authentication-
key privacy privacy-protocol privacy-key [hash | hash2]
                    - no authentication
                    - group group-name
                    - no group
            - user-template {tacplus_default | radius_default}
                - [no] access [ftp] [console] [scp-sftp] [console-port-cli] [ssh-cli] [telnet-
cli]
                - 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
                - [no] save-when-restricted
```

3.11.1.2.9 CLI script authorization commands

```
config
```

```
- system
        - security
            - cli-script
                - authorization
                    - cron
                        - cli-user user-name
                        - no cli-user
                    - event-handler
                        - cli-user user-name
                        - no cli-user
```

3.11.1.2.10 RADIUS commands

```
config
- system
        - security
            - [no] radius
                - access-algorithm {direct | round-robin}
                - [no] access-algorithm
                - [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
                - use-default-template
```

3.11.1.2.11 TACACS+ 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
                - timeout seconds
                - no timeout
                - [no] shutdown
                - [no] use-default-template
```

3.11.1.2.12 802.1x commands

```
config
- system
        - security
```

```
            - [no] dot1x
                - [no] 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]
                    - no server server-index
                    - source-address ip-address
                    - no source-address
                    - [no] shutdown
                    - timeout seconds
                    - no timeout
                - [no] shutdown
```

3.11.1.2.13 SSH commands

```
config
- system
        - security
            - ssh
                - client-cipher-list
                    - cipher index name cipher-name
                    - no cipher index
                - client-kex-list
                    - kex index name kex-name
                    - no kex index
                - client-mac-list
                    - mac index name mac-name
                    - no mac index
                - key-re-exchange
                    - client
                        - mbytes {mbytes | disable}
                        - no mbytes
                        - minutes {minutes | disable}
                        - no minutes
                        - [no] shutdown
                    - server
                        - mbytes {mbytes | disable}
                        - no mbytes
                        - minutes {minutes | disable}
                        - no minutes
                        - [no] shutdown
                - listening-port port
                - no listening-port
                - [no] preserve-key
                - server-cipher-list
                    - cipher index name cipher-name
                    - no cipher index
                - server-kex-list
                    - kex index name kex-name
                    - no kex index
                - server-mac-list
                    - mac index name mac-name
                    - no mac index
                - [no] server-shutdown
```

3.11.1.2.14 TLS commands

```
config
    system
        security
            tls
               cert-profile profile-name [create]
               no cert-profile profile-name
                   entry entry-id [create]
                   no entry entry-id
                        cert cert-filename
                        no cert
                        key key-filename
                        no key
                        [no] send-chain
                            [no] ca-profile name
                    [no] shutdown
            client-cipher-list name [create]
            no client-cipher-list name
                cipher index name cipher-suite-code
                no cipher index
                tls13-cipher index name cipher-suite-code
                no tls13-cipher index
            client-group-list name [create]
            no client-group-list name
                tls13-group index name group-suite-code
                no tls13-group index
            client-signature-list name [create]
            no client-signature-list name
                tls13-signature  index name signature-suite-code
                no tls13-signature  index
            client-tls-profile name [create]
            no client-tls-profile name
                cert-profile name
                no cert-profile
                cipher-list name
                no cipher-list
                group-list name
                no group-list
                protocol-version TLS version
                no protocol-version
                [no] shutdown
                signature-list name
                no signature-list
                trust-anchor-profile name
                no trust-anchor-profile
            trust-anchor-profile name [create]
            no trust-anchor-profile name
                [no] trust-anchor ca-profile-name
```

3.11.1.2.15 Keychain authentication commands

```
config
- system
        - security
            - [no] keychain keychain-name
                - description description-string
                - no description
                - direction
```

```
                    - bi
                        - entry entry-id [key authentication-key | hash-key | hash2-key [hash |
hash2] algorithm algorithm]
                        - no entryentry-id
                                - begin-time date hours-minutes [UTC]
                                - begin-time {now | forever}
                                - no begin-time
                                - option {basic | isis-enhanced}
                                - no option
                                - [no] shutdown
                                - tolerance {seconds | forever}
                                - no tolerance
                    - 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}
                                - no tolerance
                        - 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
                    - no receive
                    - send option-number
                    - no send
```

3.11.1.2.16 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
                - [no] disable-graceful-shutdown
                - inbound-max-sessions value
                - no inbound-max-sessions
```

```
                - outbound-max-sessions value
                - no outbound-max-sessions
                - ttl-security min-ttl-value
                - no ttl-security
            - telnet
                - [no] enable-graceful-shutdown
                - inbound-max-sessions value
                - no inbound-max-sessions
                - outbound-max-sessions value
                - no outbound-max-sessions
                - ttl-security min-ttl-value
                - no ttl-security
```

3.11.1.3 Show commands

3.11.1.3.1 Security commands

```
show
- system
        - security
            - access-group [group-name]
            - authentication [statistics]
            - communities
            - cpm-filter
                - ip-filter [entry entry-id]
                - ipv6-filter [entry entry-id]
            - keychain [keychain] [detail]
            - management-access-filter
                - ip-filter [entry entry-id]
                - ipv6-filter [entry entry-id]
            - password-options
            - profile user-profile-name
            - source-address
            - ssh
            - tls
                - cert-profile name association
                - cert-profile [name]
                - cert-profile name entry 1..8
                - client-tls-profile [client-tls-profile]
                - client-tls-profile client-tls-profile association
                - client-tls-profile client-tls-profile [connections]
                - trust-anchor-profile trust-anchor-profile association
                - trust-anchor-profile [trust-anchor-profile]
            - user [user-id] detail
            - user [user-id] lockout
            - view [view-name] [detail] [capabilities]
```

3.11.1.3.2 Login control commands

```
show
- users
```

3.11.1.4 Clear commands

3.11.1.4.1 Admin commands

```
admin
    - clear
        - lockout all
        - lockout user user-name
        - password-history all
        - password-history user user-name
```

3.11.1.4.2 Authentication commands

```
clear
- router
        - authentication
            - statistics [interface ip-int-name | ip-address]
```

3.11.1.5 Monitor commands

```
monitor
- cpm-filter
        - ip entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
        - ipv6 entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
        - mac entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
- management-access-filter
        - ip entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
        - ipv6 entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
        - mac entry entry-id [interval seconds] [repeat repeat] [absolute | rate]
```

3.11.1.6 Debug commands

```
debug
- radius [detail] [hex]
- no radius
```

3.11.2 Command descriptions

- Admin commands
- Configuration commands
- Show commands
- Clear commands
- Monitor commands
- Debug commands

3.11.2.1 Admin commands

system-password

Syntax

system-password admin-password

Context

admin>system>security

Description

This operational command changes a local administrative password.

When invoked, the user is prompted to enter the old password, the new password, and then the new password again to verify the correct input. Any subsequent invocation of **enable-admin** will require this new **admin-password**.

Parameters

admin-password

specifies to change the administrative password which is requested when a user tries to enable admin mode by running **enable-admin** to attain administrative privileges

3.11.2.2 Configuration commands

- Generic security commands
- Security commands
- Management access filter commands
- CPM filter commands
- Global password commands
- Password commands
- Profile management commands

- User management commands
- CLI script authorization commands
- RADIUS client commands
- TACACS+ client commands
- 802.1x commands
- SSH commands
- Security TLS commands
- Keychain authentication commands
- Login control commands

3.11.2.2.1 Generic security commands

description

Syntax

description *description-string*

no description

Context

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

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

config>system>security>cpm-filter>ip-filter>entry

config>system>security>cpm-filter>ipv6-filter>entry

config>system>security>keychain

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

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

Description

This command creates a text description stored in the configuration file for a configuration context.

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

Default

n/a

Parameters

description-string

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

shutdown

Syntax

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

Context

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

config>system>security>management-access-filter>ipv6-filter

config>system>security>cpm-filter>ip-filter

config>system>security>cpm-filter>ipv6-filter

config>system>security>keychain

config>system>security>keychain>direction>bi>entry

config>system>security>keychain>direction>uni>receive>entry

config>system>security>keychain>direction>uni>send>entry

config>system>security>radius

config>system>security>tacplus

Description

This command administratively disables the entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. When disabled, an entity does not change, reset, or remove any configuration settings or statistics, other than the administrative state. Many objects must be shut down before they can be deleted.

The **no** form of the command puts an entity into the administratively enabled state. Many entities must be explicitly enabled using the no shutdown command.

Default

no shutdown

3.11.2.2.2 Security commands

security

Syntax

security

Context

config>system

Description

This command enables the context to configure security settings.

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

copy

Syntax

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

Context

config>system>security

Description

This command copies the specified user or profile configuration parameters to another (destination) user or profile.

The password is set to the Return key and a new password at login must be selected.

Parameters

source-user

the user to copy from. The user must already exist.

source-profile

the profile to copy from. The profile must already exist.

destination

the destination user or profile

overwrite

specifies that the destination user or profile configuration will be overwritten with the copied source user or profile configuration. A configuration will not be overwritten if the overwrite command is not specified.

ftp-server

Syntax

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

Context

config>system>security

Description

This command enables FTP servers running on the system.

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

The **no** form of the 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

Description

Whenever the user executes a save or info command, the system will encrypt all passwords, 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 wants to configure the same password. However, because it is the same password and the hash key is limited to the password/key, it is obvious that it is the same key.

The second algorithm is a more complex key, and cannot be copied and pasted in different locations in the configuration file. In this case, if the same key or password is used repeatedly in different contexts, each encrypted (hashed) version will be different.

Default

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

Parameters

read-version {1 | 2 | all}

when the read-version is configured as "all," both versions 1 and 2 will be accepted by the system. Otherwise, only the selected version will be accepted when reading configuration or exec files. The presence of incorrect hash versions will abort the script/startup.

write-version {1 | 2}

selects the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.

source-address

Syntax

source-address

Context

config>system>security

Description

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

application

Syntax

application *app* [*ip-int-name* | *ip-address*]

no application *app*

Context

config>system>security>source-address

Description

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

The **no** form of the command removes the specified source address from the application, causing the application to use the system IP address as the source address.

Parameters

app

specifies the application name

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

ip-int-name | *ip-address*

specifies the name of the IP interface or IPv4 address. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

application6

Syntax

application6 *app ipv6-address*

no application6 *app*

Context

config>system>security>source-address

Description

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

The **no** form of the command removes the specified source address from the application, causing the application to use the system IP address as the source address.

Parameters

app

specifies the application name

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

ipv6-address

specifies the IPv6 address

telnet

Syntax

telnet

Context

config>system>security

Description

This command enables the context to configure Telnet parameters.

listening-port

Syntax

listening-port *port*

no listening-port

Context

config>system>security>telnet

Description

This command configures the listening TCP port of the Telnet server for incoming Telnet connections via base or management routing. VPRN node management is done via GRT leaking and uses base routing.

The **no** form of this command resets the listening port to its default of 23.

Default

no listening port

Parameters

port

specifies the port number

Values 1024 to 49151

telnet-server

Syntax

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

Context

config>system>security

Description

This command enables Telnet servers running on the system.

Telnet servers are off by default. At system startup, only SSH servers are enabled.

Telnet servers in 7705 SAR networks limit a Telnet client to three retries to log in. The Telnet server disconnects the Telnet client session after three retries.

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

Default

no telnet-server

telnet6-server

Syntax

[**no**] **telnet6-server**

Context

config>system>security

Description

This command enables Telnet IPv6 servers running on the system.

Telnet servers are off by default. At system startup, only SSH servers are enabled.

Telnet servers in 7705 SAR networks limit a Telnet client to three retries to log in. The Telnet server disconnects the Telnet client session after three retries.

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

Default

no telnet6-server

vprn-network-exceptions

Syntax

vprn-network-exceptions [*number seconds*]

no vprn-network-exceptions

Context

config>system>security

Description

This command configures the rate at which the 7705 SAR sends ICMP replies to a source IP address in response to TTL expiry IP packets that have been received for all VPRN instances in the system and from all network IP interfaces. Packets include labeled user packets as well as ping and traceroute packets within a VPRN.

This command does not apply to MPLS packets or service OAM packets such as VPRN ping and trace, LSP ping and trace, and VCC ping and trace.

When the command is issued without any *number* and *seconds* parameters specified, the default rate is 100 ICMP reply packets sent per 10 seconds. The **no** form of the command disables the rate-limiting of ICMP replies.

Default

no vprn-network-exceptions

Parameters

number

specifies the maximum number of ICMP reply messages that can be sent within the configured number of seconds

Values 10 to 1000

seconds

specifies the time frame in which the configured number of ICMP reply messages can be sent

Values 1 to 60

3.11.2.2.3 Management access filter commands

management-access-filter

Syntax

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

Context

config>system>security

Description

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

Management access filters control all traffic in and out of the CSM. They can be used to restrict management of the 7705 SAR by other nodes outside either specific (sub)networks or through designated ports.

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

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

Default

n/a

ip-filter

Syntax

ip-filter

Context

config>system>security>management-access-filter

Description

This command enables the context to configure IP filter commands.

ipv6-filter

Syntax

ipv6-filter

Context

config>system>security>management-access-filter

Description

This command enables the context to configure IPv6 filter commands.

default-action

Syntax

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

Context

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

config>system>security>management-access-filter>ipv6-filter

Description

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

The **default-action** is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the **default-action** must be defined.

Default

n/a

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 will be denied

deny-host-unreachable

specifies that packets not matching the selection criteria will be denied and a host unreachable message will be issued

entry

Syntax

[**no**] **entry**

Context

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

config>system>security>management-access-filter>ipv6-filter

Description

This command is used to create or edit a management access filter entry. Multiple entries can be created with unique *entry-id* numbers. The 7705 SAR exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.

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

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

Default

n/a

Parameters

entry-id

an entry ID uniquely identifies a match criteria and the corresponding action. It is recommended 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>management-access-filter>ip-filter>entry

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

Description

This command creates the action associated with the management access filter match criteria entry.

The **action** keyword is required. If no action is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.

If the packet does not meet any of the match criteria, the configured default action is applied.

Default

n/a

Parameters

permit

specifies that packets matching the configured criteria will be permitted

deny

specifies that packets not matching the selection criteria will be denied

deny-host-unreachable

specifies that packets not matching the selection criteria will be denied and a host unreachable message will be issued

dst-port

Syntax

dst-port *port* [*mask*]

no dst-port

Context

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

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

Description

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

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

Default

n/a

Parameters

port

the source TCP or UDP port number as match criteria

Values 1 to 65535 (decimal)

mask

mask used to specify a range of destination port numbers as the match criterion

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

Table 8: 16-bit mask formats

Format style	Format syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBBB	0b1111100000000000

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

Values 1 to 65535 (decimal)

Default 65535 (exact match)

flow-label

Syntax

flow-label *value*

no flow-label

Context

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

Description

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

This command applies to IPv6 filters only.

Parameters

value

the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (see RFC 3595, *Textual Conventions for IPv6 Flow Label*)

Values 0 to 1048575

log

Syntax

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

Context

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

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

Description

This command enables match logging.

The **no** form of this command disables match logging.

Default

no log

next-header

Syntax

[**no**] **next-header** *next-header*

Context

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

Description

This command specifies the next header to match as a management access filter match criterion.

This command applies to IPv6 filters only.

Parameters

next-header

protocol-number or *protocol-name*

protocol-number

the IPv6 next header to match, expressed as a protocol number in decimal, hexadecimal, or binary. This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria. See Table 9: IP protocol IDs and descriptions for the protocol IDs and descriptions for the IP protocols.

Values [0 to 255]D

[0x0 to 0xFF]H

[0b0 to 0b11111111]B

protocol-name

the IPv6 next header to match, expressed as a protocol name. This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria. See Table 9: IP protocol IDs and descriptions for the protocol IDs and descriptions for the IP protocols.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

protocol

Syntax

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

Context

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

Description

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

The protocol type is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17). The following table lists the protocol IDs and descriptions for the IP protocols.

Table 9: IP protocol IDs and descriptions

Protocol ID	Protocol	Description
1	icmp	Internet Control Message
2	igmp	Internet Group Management
4	ip	IP in IP (encapsulation)
6	tcp	Transmission Control
8	egp	Exterior Gateway Protocol
9	igp	Any private interior gateway
17	udp	User Datagram
27	rdp	Reliable Data Protocol
41	ipv6	IPv6
43	ipv6-route	Routing Header for IPv6
44	ipv6-frag	Fragment Header for IPv6
45	idrp	Inter-Domain Routing Protocol
46	rsvp	Reservation Protocol
47	gre	General Routing Encapsulation
58	ipv6-icmp	ICMP for IPv6
59	ipv6-no-nxt	No Next Header for IPv6
60	ipv6-opts	Destination Options for IPv6
80	iso-ip	ISO Internet Protocol
88	eigrp	EIGRP
89	ospf-igp	OSPFIGP
97	ether-ip	Ethernet-within-IP Encapsulation
98	encap	Encapsulation Header
102	pnni	PNNI over IP

Protocol ID	Protocol	Description
103	pim	Protocol Independent Multicast
112	vrrp	Virtual Router Redundancy Protocol
115	l2tp	Layer Two Tunneling Protocol
118	stp	Schedule Transfer Protocol
123	ptp	Performance Transparency Protocol
124	isis	ISIS over IPv4
126	crtp	Combat Radio Transport Protocol
127	crudp	Combat Radio User Datagram
132	sctp	Stream Control Transmission Protocol
137	mpls-in-ip	MPLS in IP

This command applies to IPv4 filters only.

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

Default

n/a

Parameters

protocol-id

protocol-number or *protocol-name*

protocol-number

the protocol number for the match criterion, expressed in decimal, hexadecimal, or binary

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name

the protocol name for the match criterion

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

router

Syntax

router *router-instance*

router service-name *service-name*

no router

Context

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

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

Description

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

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

Parameters

router-instance

specifies one of the following parameters for the router instance:

router-name – specifies a router name up to 32 characters to be used in the match criteria

service-id – specifies an existing service ID to be used in the match criteria

Values 1 to 2147483647

service-name

specifies the service name of an existing service

Values up to 64 characters

src-ip

Syntax

src-ip {*ip-prefix*[*/mask*] [*I netmask*]| **ip-prefix-list** *ip-prefix-list-name*}

no src-ip

Context

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

Description

This command specifies a source IPv4 address range or specifies an IPv4 prefix list configured under the **match-list** command to be used as a match criterion for a management access filter. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the source IP address, specify the address and the associated mask (for example, 10.1.0.0/16). The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of the command removes the source IPv4 address or IPv4 prefix list match criterion.

Default

n/a

Parameters

ip-prefix

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

Values a.b.c.d (host bits must be 0)

mask

the subnet mask length expressed as a decimal integer

Values 1 to 32

netmask

the subnet mask in dotted-decimal notation

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

ip-prefix-list-name

the name of the IP prefix list configured with the **match-list** command

src-ip

Syntax

src-ip {*ipv6-address/prefix-length* | **ipv6-prefix-list** *ipv6-prefix-list-name*}

no src-ip

Context

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

Description

This command configures a source IPv6 address range or specifies an IPv6 prefix list configured under the **match-list** command to be used as a match criterion for a management access filter. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the source IP address, specify the address and prefix length; for example, 11::12/128.

The **no** form of the command removes the source IP address or IPv6 prefix list match criterion.

Default

n/a

Parameters

ipv6-address/prefix-length

the IPv6 address on the interface

Values *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 to FFFF]H
d: [0 to 255]D
prefix-length: 1 to 128

ipv6-prefix-list-name

the name of the IPv6 prefix list configured with the **match-list** command

src-port

Syntax

src-port {*port-id* | **cpm** | **lag** *lag-id*}

no src-port

Context

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

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

Description

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

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

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

Default

any interface

Parameters

port-id

the port ID

Values port-id *slot*/*mda*/*port*

bundle-id	**bundle**-*type*-*slot*/*mda*.*bundle-num*	
	type	**ima**, **ppp**
	bundle-num	1 to 128

cpm

specifies that ingress management traffic is restricted to the CSM Ethernet port

lag-id

the LAG ID

Values 1 to 32

renum

Syntax

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

Context

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

config>system>security>management-access-filter>ipv6-filter

Description

This command renumbers existing management access filter entries to resequence filter entries.

The 7705 SAR 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 from most to least explicit.

Parameters

old-entry-number

the entry number of the existing entry

Values 1 to 9999

new-entry-number

the new entry number that will replace the old entry number

Values 1 to 9999

3.11.2.2.4 CPM filter commands

cpm-filter

Syntax

[**no**] **cpm-filter**

Context

config>system>security

Description

This command enables the context to configure a CPM (referred to as CSM on the 7705 SAR) filter. A CPM filter is a hardware filter (that is, implemented on the network processor) for the CSM-destined traffic that applies to all the traffic destined for the CSM CPU. It can be used to drop or accept packets, as well as allocate dedicated hardware queues for the traffic. The hardware queues are not user-configurable.

The **no** form of the command disables the CPM filter.

default-action

Syntax

default-action {**accept** | **drop**}

Context

config>system>security>cpm-filter

Description

This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP filter entries of the filter. If there are no filter entries defined, the packets received is either accepted or dropped based on that default action.

Default

accept

Parameters

accept

packets are accepted unless there is a specific filter entry that causes the packet to be dropped

drop

packets are dropped unless there is a specific filter entry that causes the packet to be accepted

ip-filter

Syntax

ip-filter

Context

config>system>security>cpm-filter

Description

This command enables the context to configure IPv4 CPM filter parameters.

ipv6-filter

Syntax

ipv6-filter

Context

config>system>security>cpm-filter

Description

This command enables the context to configure IPv6 CPM filter parameters.

entry

Syntax

entry *entry-id* [**create**]

no entry *entry-id*

Context

config>system>security>cpm-filter>ip-filter

config>system>security>cpm-filter>ipv6-filter

Description

This command specifies a particular CPM filter match entry. Every CPM filter must have at least one filter match entry. A filter entry with no match criteria set matches every packet, and the entry action is taken.

The **create** keyword must be used with every new entry configured. After the entry has been created, you can navigate to the entry context without using the **create** keyword.

All IPv4 filter entries can specify one or more matching criteria. There are no range-based restrictions on any IPv4 filter entries.

For IPv6 filters, the combined number of fields for all entries in a filter must not exceed 16 fields (or 256 bits), where a field contains the bit representation of the matching criteria.

Parameters

entry-id

identifies a CPM filter entry as configured on this system.

Values 1 to 64

action

Syntax

action {**accept** | **drop**}

no action

Context

config>system>security>cpm-filter>ip-filter>entry

config>system>security>cpm-filter>ipv6-filter>entry

Description

This command specifies the action to take for packets that match this filter entry.

Default

drop

Parameters

accept

packets matching the entry criteria are forwarded

drop

packets matching the entry criteria are dropped

log

Syntax

log *log-id*

no log

Context

config>system>security>cpm-filter>ip-filter>entry

config>system>security>cpm-filter>ipv6-filter>entry

Description

This command specifies the log in which packets matching this entry should be entered. The value 0 indicates that logging is disabled.

The **no** form of the command deletes the log ID.

Parameters

log-id

the log ID where packets matching this entry should be entered

Values 101 to 199

match

Syntax

match [**protocol** *protocol-id*]

no match

Context

config>system>security>cpm-filter>ip-filter>entry

Description

This command enables the context to enter match criteria for the IPv4 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.

A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.

This command also optionally specifies the IP protocol to be used as an IP filter match criterion. See Table 9: IP protocol IDs and descriptions .

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

Parameters

protocol-id

protocol-number or *protocol-name*

protocol-number

the protocol number in decimal, hexadecimal, or binary, to be used as an IP filter match criterion

Values [0 to 255]D

[0x0 to 0xFF]H

[0b0 to 0b11111111]B

protocol-name

the protocol name to be used as an IP filter match criterion

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

match

Syntax

match [**next-header** *next-header*]

no match

Context

config>system>security>cpm-filter>ipv6-filter>entry

Description

This command enables the context to enter match criteria for the IPv6 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.

A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.

This command also optionally specifies the IPv6 next header (protocol number or protocol name) to be used as an IPv6 match criterion. See Table 9: IP protocol IDs and descriptions .

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

Parameters

next-header

protocol-number or *protocol-name*

protocol-number

the IPv6 next header to match, expressed as a protocol number in decimal, hexadecimal, or binary. This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria.

Values [1 to 42 | 45 to 49 | 52 to 59 | 61 to 255]D

[0x0 to 0x2A | 0x2D to 0x31 | 0x34 to 0x3B | 0x3D to 0xFF]H

[0b0 to 0b101010 | 0b101101 to 0b110001 | 0b110100 to 0b111011 | 0b111101 to 0b11111111]B

protocol-name

the IPv6 next header to match, expressed as a protocol name. This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

dscp

Syntax

dscp *dscp-name*

no dscp

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

The **no** form of the command removes the DSCP match criterion.

Default

no dscp

Parameters

dscp-name

a DSCP name that has been previously mapped to a value using the dscp-name command. The DiffServ Code Point can only be specified by its name.

Values be|cp1|cp2|cp3|cp4|cp5|cp6|cp7|cs1|cp9|af11|cp11|
af12|cp13|af13|cp15|cs2|cp17|af21|cp19|af22|cp21|
af23|cp23|cs3|cp25|af31|cp27|af32|cp29|af33|cp31|cs4|
cp33|af41|cp35|af42|cp37|af43|cp39|cs5|cp41|cp42|
cp43|cp44|cp45|ef|cp47|nc1|cp49|cp50|cp51|cp52|cp53|
cp54|cp55|nc2|cp57|cp58|cp59|cp60|cp61|cp62|cp63

dst-ip

Syntax

dst-ip {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}

no dst-ip

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

This command configures a destination IPv4 address range or specifies an IPv4 prefix list configured under the **match-list** command to be used as an IP filter match criterion. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the destination IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of the command removes the destination IPv4 address or IPv4 prefix list match criterion.

Default

no dst-ip

Parameters

ip-address

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

Values 0.0.0.0 to 255.255.255.255

mask

the subnet mask length expressed as a decimal integer

Values 1 to 32

ipv4-address-mask

the dotted-decimal equivalent of the mask length

Values 0.0.0.0 to 255.255.255.255

prefix-list-name

the name of the IPv4 prefix list configured with the **match-list** command

dst-ip

Syntax

dst-ip {*ipv6-address/prefix-length* | **ipv6-prefix-list** *ipv6-prefix-list-name*}

no dst-ip

Context

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures a destination IPv6 address range or specifies an IPv6 prefix list configured under the **match-list** command to be used as an IP filter match criterion. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the destination IP address, specify the address and prefix length; for example, 11::12/128.

The **no** form of the command removes the destination IPv6 address or IPv6 prefix list match criterion.

Default

n/a

Parameters

ipv6-address/prefix-length

the IPv6 address on the interface

Values *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 to FFFF]H
d: [0 to 255]D
prefix-length: 1 to 128

ipv6-prefix-list-name

the name of the IPv6 prefix list configured with the **match-list** command

dst-port

Syntax

dst-port *tcp/udp port-number* [*mask*]

no dst-port

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command specifies the TCP/UDP port to match the destination port of the packet.

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

The TCP or UDP protocol must be configured using the match command before this filter can be configured.

Parameters

tcp/udp port-number

the destination port number to be used as a match criterion

Values [0 to 65535]D
[0x0 to 0xFF]H
[0b0 to 0b1111111111111111]B

mask

the 16-bit mask to be applied when matching the destination port

Values [0 to 65535]D
[0x0000 to 0xFFFF]H
[0b0000000000000000 to 0b1111111111111111]B

fragment

Syntax

fragment {**true** | **false**}

no fragment

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

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

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

This command applies to IPv4 filters only.

Default

false

Parameters

true

configures a match on all fragmented IP packets. A match occurs 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

configures a 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.

icmp-code

Syntax

icmp-code *icmp-code*

no icmp-code

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures matching on an ICMP code field in the ICMP header of an IP packet as an IP filter match criterion.

The ICMP protocol must be configured using the match command before this filter can be configured.

The **no** form of the command removes the criterion from the match entry.

Default

no icmp-code

Parameters

icmp-code

icmp-code-number or *icmp-code-keyword*

icmp-code-number

the ICMP code number in decimal, hexadecimal, or binary, to be used as a filter match criterion

Values [0 to 255]D

[0x0 to 0xFF]H

[0b0 to 0b11111111]B

icmp-code-keyword

the ICMP code keyword to be used as a filter match criterion

Values **For IPv4 filter**: none, network-unreachable, host-unreachable, protocol-unreachable, port-unreachable, fragmentation-needed, source-route-failed, dest-network-unknown, dest-host-unknown, src-host-isolated, network-unreachable-for-tos, host-unreachable-for-tos

For IPv6 filter: none, no-route-to-destination, comm-with-dest-admin-prohibited, beyond-scope-src-addr, address-unreachable, port-unreachable

icmp-type

Syntax

icmp-type *icmp-type*

no icmp-type

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures matching on an ICMP type field in the ICMP header of an IP packet as an IP filter match criterion.

The ICMP protocol must be configured using the match command before this filter can be configured.

The **no** form of the command removes the criterion from the match entry.

Default

no icmp-type

Parameters

icmp-type

icmp-type-number or *icmp-type-keyword*

icmp-type-number

the ICMP type number in decimal, hexadecimal, or binary, to be used as a match criterion

Values [0 to 255]D

[0x0 to 0xFF]H

[0b0 to 0b11111111]B

icmp-type-keyword

the ICMP type keyword to be used as a match criterion

Values **For IPv4 filter**: none, echo-reply, dest-unreachable, source-quench, redirect, echo-request, router-advt, router-selection, time-exceeded, parameter-problem, timestamp-request, timestamp-reply, addr-mask-request, addr-mask-reply, photuris

For IPv6 filter: none, dest-unreachable, packet-too-big, time-exceeded, parameter-problem, echo-request, echo-reply, multicast-listen-query, multicast-listen-report, multicast-listen-done, router-solicitation, router-advt, neighbor-solicitation, neighbor-advertisement, redirect-message, router-renumbering, icmp-node-info-query, icmp-node-info-resp, inv-nd-solicitation, inv-nd-adv-message, multicast-listener-report-v2, home-agent-ad-request, home-agent-ad-reply, mobile-prefix-solicitation, mobile-prefix-advt, cert-path-solicitation, cert-path-advt, multicast-router-advt, multicast-router-solicitation, multicast-router-termination, fmipv6, rpl-control, ilnpv6-locator-update, duplicate-addr-request, duplicate-addr-confirmation

ip-option

Syntax

ip-option *ip-option-value* [*ip-option-mask*]

no ip-option

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

This command configures matching packets with a specific IP option or a range of IP options in the IP header as an IP filter match criterion.

The option type octet contains 3 fields:

- 1 bit copied flag (copy options in all fragments)
- 2 bits option class
- 5 bits option number

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

This command applies to IPv4 filters only.

Default

no ip-option

Parameters

ip-option-value

the 8-bit option type (can be entered using decimal, hexadecimal, or binary formats). The mask is applied as an AND to the option byte and the result is compared with the option value.

The decimal value entered for the match should be a combined value of the 8-bit option type field and not just the option number. Therefore, to match on IP packets that contain the Router Alert option (option number = 20), enter the option type of 148 (10010100).

Values 0 to 255

ip-option-mask

specifies a range of option numbers to use as the match criteria

This 8-bit mask can be entered using decimal, hexadecimal, or binary formats as shown in the following table.

Table 10: IP option formats

Format style	Format syntax	Example
Decimal	DDD	20

Format style	Format syntax	Example
Hexadecimal	0xHH	0x14
Binary	0bBBBBBBBB	0b0010100

Values 0 to 255

Default 255 (decimal) (exact match)

multiple-option

Syntax

multiple-option {**true** | **false**}

no multiple-option

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

This command configures matching packets that contain more than one option field in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the number of option fields in the IP header as a match criterion.

This command applies to IPv4 filters only.

Default

no multiple-option

Parameters

true

specifies matching on IP packets that contain more than one option field in the header

false

specifies matching on IP packets that do not contain multiple option fields in the header

option-present

Syntax

option-present {**true** | **false**}

no option-present

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

This command configures matching packets that contain the option field or have an option field of 0 in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the option field in the IP header as a match criterion.

This command applies to IPv4 filters only.

Parameters

true

specifies matching on all IP packets that contain the option field in the header. A match occurs for all packets that have the option field present. An option field of 0 is considered as no option present.

false

specifies matching on IP packets that do not have any option field present in the IP header (an option field of 0)

src-ip

Syntax

src-ip {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}

no src-ip

Context

config>system>security>cpm-filter>ip-filter>entry>match

Description

This command specifies the IPv4 address or specifies an IPv4 prefix list configured under the **match-list** command to be used as a match criterion for an IP filter. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the source IPv4 address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of the command removes the source IPv4 address or IPv4 prefix list match criterion.

Default

no src-ip

Parameters

ip-address

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

Values 0.0.0.0 to 255.255.255.255

mask

the subnet mask length expressed as a decimal integer

Values 1 to 32

ipv4-address-mask

the dotted-decimal equivalent of the mask length

Values 0.0.0.0 to 255.255.255.255

prefix-list-name

the name of the IPv4 prefix list configured with the **match-list** command

src-ip

Syntax

src-ip {*ipv6-address/prefix-length* | **ipv6-prefix-list** *ipv6-prefix-list-name*}

no src-ip

Context

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures a source IPv6 address range or specifies an IPv6 prefix list configured under the **match-list** command to be used as a match criterion for an IP filter. See the 7705 SAR Router Configuration Guide for information about the **match-list** command.

To match on the source IP address, specify the address and prefix length; for example, 11::12/128.

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

Default

n/a

Parameters

ipv6-address/prefix-length

the IPv6 address on the interface

Values *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 to FFFF]H
d: [0 to 255]D
prefix-length 1 to 128

ipv6-prefix-list-name

the name of the IPv6 prefix list configured with the **match-list** command

src-port

Syntax

src-port *tcp/udp port-number* [*mask*]

no src-port

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command specifies the TCP/UDP port to match the source port of the packet.

Default

no src-port

Parameters

tcp/udp port-number

the source port number to be used as a match criterion

Values [0 to 65535]D
[0x0 to 0xFF]H
[0b0 to 0b1111111111111111]B

mask

the 16-bit mask to be applied when matching the source port

Values [0 to 65535]D
[0x0000 to 0xFFFF]H
[0b0000000000000000 to 0b1111111111111111]B

tcp-ack

Syntax

tcp-ack {**true** | **false**}

no tcp-ack

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.

The no form of the command removes the criterion from the match entry.

Default

no tcp-ack

Parameters

true

specifies matching on IP packets that have the ACK bit set in the control bits of the TCP header of an IP packet

false

specifies matching on IP packets that do not have the ACK bit set in the control bits of the TCP header of the IP packet

tcp-syn

Syntax

tcp-syn {**true** | **false**}

no tcp-syn

Context

config>system>security>cpm-filter>ip-filter>entry>match

config>system>security>cpm-filter>ipv6-filter>entry>match

Description

This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.

The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP address.

The **no** form of the command removes the criterion from the match entry.

Default

no tcp-syn

Parameters

true

specifies matching on IP packets that have the SYN bit set in the control bits of the TCP header

false

specifies matching on IP packets that do not have the SYN bit set in the control bits of the TCP header

renum

Syntax

renum old-entry-id new-entry-id

Context

config>system>security>cpm-filter>ip-filter

config>system>security>cpm-filter>ipv6-filter

Description

This command renumbers existing IP filter entries to resequence filter entries.

Resequencing may be required in some cases because the process is exited when the first match is found and the actions are executed according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters

old-entry-id

the entry number of an existing entry

Values 1 to 64

where: 1 to 29 are filter entries

30 to 64 are extended filter entries

new-entry-id

the new entry number to be assigned to the old entry

Values 1 to 64

where: 1 to 29 are filter entries

30 to 64 are extended filter entries

3.11.2.2.5 Global password commands

enable-admin

Syntax

enable-admin

Context

<global>

Description

Note: See the description for the admin-password command. If the **admin-password** is configured in the **config>system>security>password** context, 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 have access to this command.

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

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

- enter the **show users** command – the administrator can see which users are in enable-admin mode, indicated by the "A" on the same line as that username
- enter the **enable-admin** command again at the root prompt and an error message is returned

The # sign indicates the current session.

```
A:7705:Dut-C# show users
===============================================================================
Username                                        Type
    From
    Router instance
    Connection ID                               Login time
        Session ID            SSH Channel ID        Idle time
===============================================================================
                                                Console
    --
    --
    6                                                --
        6                     --                    0d 00:03:20  --
-------------------------------------------------------------------------------
admin                                           Telnet
    192.168.192.37
    management
    8                                           03OCT2023 14:06:52
        8                     --                    0d 00:01:04  --
-------------------------------------------------------------------------------
bla                                             Telnet
    192.168.192.37
    management
    9                                           03OCT2023 14:08:42
        9                     --                    0d 00:00:09  A-
-------------------------------------------------------------------------------
admin                                           SSHv2
    192.168.192.37
    management
    7                                           03OCT2023 14:06:24
       #7                     0                     0d 00:00:00  --
-------------------------------------------------------------------------------
Number of users: 3
Number of sessions: 3
'#' indicates the current active session
'A' indicates user is in admin mode
===============================================================================
*A:7705:Dut-C#
```

3.11.2.2.6 Password commands

password

Syntax

password

Context

config>system>security

Description

This command enables the context to configure password management parameters.

admin-password

Syntax

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

no admin-password

Context

config>system>security>password

Description

This command allows a user (with admin permissions) to configure a password which enables a user to become an administrator for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.

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

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

Note: 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 are 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@192.0.2.0/test/srcfile cf3:\destfile

In this example, the username "test" and password "secret" are not sent to the AAA servers (or to any logs). They are replaced with "****".

Note: See the description for the system-password command. Any user that either has administrative privileges or has entered **enable-admin** mode can run the **admin>system>security>system-password admin-password** command to change this admin-password as required.

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

Default

no admin-password

Parameters

password

configures the password that enables a user to become a system administrator. The maximum length is as follows:

- 56 characters if in unhashed plaintext

  The unhashed plaintext form must meet all the requirements that are defined within the complexity-rules command context.
- 60 characters if hashed with bcrypt
- from 87 to 92 characters if hashed with PBKDF2 SHA-2
- from 131 to 136 characters if hashed with PBKDF2 SHA-3
- 32 characters if the **hash** keyword is specified
- 54 characters if the **hash2** keyword is specified

hash

specifies that the key is entered and stored on the node in encrypted form

hash2

specifies that the key is entered and stored on the node in a more complex encrypted form

Note: If neither the **hash** nor **hash2** keyword is specified, the key is entered in clear text. However, for security purposes, the key is stored on the node using bcrypt or PBKDF2 hash encryption.

aging

Syntax

aging *days*

no aging

Context

config>system>security>password

Description

This command configures the number of days a user password is valid before the user must change their password.

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

Default

no aging is enforced

Parameters

days

the maximum number of days the password is valid

Values 1 to 500

attempts

Syntax

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

no attempts

Context

config>system>security>password

Description

This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.

If the threshold is exceeded, the user is locked out for a specified time period.

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

The **no attempts** command resets all values to the default.

Default

count: 3 minutes1: 5 minutes2: 10

Parameters

count

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

Values 1 to 64

minutes1

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

minutes2

the lockout period, in minutes, where the user is not allowed to log in

Values 0 to 1440

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

authentication-order

Syntax

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

no authentication-order

Context

config>system>security>password

Description

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

The order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.

If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log registers the failed attempt. Both the attempted login identification and originating IP address are logged with a timestamp.

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

Default

authentication-order radius tacplus local

Parameters

method-1

the first password authentication method to attempt

Values radius, tacplus, local

Default radius

method-2

the second password authentication method to attempt

Values radius, tacplus, local

Default tacplus

method-3

the third password authentication method to attempt

Values radius, tacplus, local

Default local

radius

RADIUS authentication

tacplus

TACACS+ authentication

local

password authentication based on the local password database

exit-on-reject

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

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

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

complexity-rules

Syntax

complexity-rules

Context

config>system>security>password

Description

This command enables the context to configure security password complexity rules.

allow-user-name

Syntax

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

Context

config>system>security>password>complexity-rules

Description

This command allows a login name to be included as part of the password.

The **no** form of this command prevents a login name from being included 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

Description

This command configures a credit value for each of the different character classes in a local password. When a password is created, credits are assigned for each character in a character class, up to the assigned *credits* limit. The credits each count as one additional character toward the minimum length of the password. This allows a trade-off between a very long, simple password and a short, complex one.

For example, if the password minimum length is seven and **lowercase** *credits* is set to 3, a password with four lowercase letters, such as "srty", is accepted. The first three lowercase letters are each given a credit worth one extra character. Combined with the four characters in the password, the total reaches the minimum length. If **lowercase** *credits* is set to 2 instead of 3, only the first two lowercase letters are given credit. In this case, the "srty" password is worth only six characters (four characters plus two extra characters from credits) and would fail to reach the seven character minimum length.

The **no** form of this command removes all credit values.

Default

no credits

Parameters

credits

the number of credits allowed for each character class

Values 0 to 10

disallow-sequence-keys

Syntax

disallow-sequence-keys *value*

no disallow-sequence-keys

Context

config>system>security>password>complexity-rules

Description

This command configures the number of consecutive characters that are not allowed to be entered as part of the password on a U.S. English or Korean keyboard. These characters can be lowercase or uppercase letters, or numbers. Special characters are not taken into account. These consecutive characters can be horizontal (left to right or right to left), diagonal (top to bottom or bottom to top), or wrapped (for example, "dsalkj" is a sequence of 6 characters). If the number of consecutive characters is equal to or larger than the configured value, the password is disallowed.

For example, if the user attempts to use the password "dsalkjhgfdsa" with this command configured to 8 (meaning any sequence of 8 or more characters fails), the system rejects the password because the substring “lkjhgfdsa” is a sequence of 9 letters and therefore does not pass the check. If the user attempts to use the password “9lkjhgfd5c”, the system accepts the password because the substring “lkjhgfd” is a sequence of 7 characters, which passes the check.

The **no** form of this command removes the restriction on the number of characters.

Default

no disallow-sequence-keys

Parameters

value

specifies the number of disallowed sequential characters in the password

Values 2 to 8

minimum-classes

Syntax

minimum-classes *minimum*

no minimum-classes

Context

config>system>security>password>complexity-rules

Description

This command enforces a minimum number of different character classes to be used in the password. The possible character classes are lowercase letters, uppercase letters, numbers, and special characters.

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

Default

no minimum-classes

Parameters

minimum

the minimum number of character classes required in a password

Values 2 to 4

minimum-length

Syntax

minimum-length *value*

no minimum-length

Context

config>system>security>password>complexity-rules

Description

This command configures the minimum number of characters required for passwords.

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

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

Default

6

Parameters

value

the minimum number of characters required for a password

Values 6 to 50

repeated-characters

Syntax

repeated-characters *count*

no repeated-characters

Context

config>system>security>password>complexity-rules

Description

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

The **no** form of the command resets to the default value, which removes the restriction on repeated characters in passwords.

Default

no repeated-characters

Parameters

count

the maximum number of consecutive repeated characters allowed in the password

Values 1 to 8

required

Syntax

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

no required

Context

config>system>security>password>complexity-rules

Description

This command configures the minimum number of characters from each character class that are required for a password to be valid.

The **no** form of the command removes the minimum required characters from each character class.

Default

no required

Parameters

count

the minimum number of characters required from the character class

Values 0 to 10

hashing

Syntax

hashing {**bcrypt** | **sha2-pbkdf2** | **sha3-pbkdf2**}

Context

config>system>security>password

Description

This command configures the password hashing algorithm.

Default

bcrypt

Parameters

bcrypt

sets the password hashing algorithm to bcrypt

sha2-pbkdf2

sets the password hashing algorithm to PBKDF2 with SHA-2 hashing

sha3-pbkdf2

sets the password hashing algorithm to PBKDF2 with SHA-3 hashing

health-check

Syntax

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

Context

config>system>security>password

Description

This command specifies that RADIUS and TACACS+ servers are monitored for 3 s each during every polling interval. Servers that are not configured have 3 s of idle time. If a server is found to be unreachable, or a previously unreachable server starts responding, depending on the type of server, a trap is sent.

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

Default

30

Parameters

interval

the polling interval for RADIUS and TACACS+ servers, in seconds

Values 6 to 1500

history-size

Syntax

history-size *size*

no history-size

Context

config>system>security>password

Description

This command configures the number of previous passwords to save in the system. A new password is matched against every old password and is rejected if it is identical to a password in the history.

The **no** form of the command prevents password history matching.

Default

no history-size

Parameters

size

specifies how many previous passwords are stored in the history

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

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

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

Values 0 to 1

hours

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

Values 0 to 23

minutes

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

Values 0 to 59

seconds

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

Description

This command configures the minimum number of characters in a new password that must be unique from the previous password.

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

Default

no minimum-change

Parameters

length

the minimum number of characters in a new password that must be unique from a previous password

Values 1 to 20

3.11.2.2.7 Profile management commands

profile

Syntax

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

Context

config>system>security

Description

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

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

After the profiles are created, the **user** 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 **no** form of the command deletes a user profile.

Default

user-profile default

Parameters

user-profile-name

the user profile name entered as a character string. The string is case-sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

default-action

Syntax

default-action {**deny-all** | **permit-all** | **none**}

Context

config>system>security>profile

Description

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

Default

none

Parameters

deny-all

sets the default of the profile to deny access to all commands

permit-all

sets the default of the profile to allow access to all commands

Note: The **permit-all** parameter does not change access to security commands. Security commands are only and always available to members of the admin-user profile.

none

sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user.

For example, if a user is a member of two profiles and the default action of the first profile is **permit-all**, then the second profile will never be evaluated because **permit-all** is executed first. If the first profile default action is set to **none** and if no match conditions are met in the first profile, then the second profile will be evaluated. If the default action of the last profile is **none** and no explicit match is found, then the default-action **deny-all** takes effect.

entry

Syntax

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

Context

config>system>security>profile

Description

This command is used to create a user profile entry.

More than one entry can be created with unique *entry-id* numbers. The 7705 SAR exits when the first match is found and executes the actions according to the accompanying action command. Entries should be sequenced from most explicit to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** for it to be considered complete.

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

Default

no entry IDs are defined

Parameters

entry-id

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

Values 1 to 9999

action

Syntax

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

Context

config>system>security>profile>entry

Description

This command configures the action associated with the profile entry.

Parameters

deny

specifies that commands matching the entry command match criteria will be denied

permit

specifies that commands matching the entry command match criteria will be permitted

match

Syntax

match *command-string*

no match

Context

config>system>security>profile>entry

Description

This command configures a command or command subtree.

Because the 7705 SAR exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile.

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

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

Default

no match command string is specified

Parameters

command-string

the CLI command or CLI tree level that is the scope of the profile entry

renum

Syntax

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

Context

config>system>security>profile

Description

This command renumbers profile entries to resequence the entries.

Because the 7705 SAR 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

the entry number of an existing entry

Values 1 to 9999

new-entry-number

the new entry number

Values 1 to 9999

3.11.2.2.8 User management commands

user

Syntax

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

Context

config>system>security

Description

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

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

When a new user is created and the **info** command is entered, the system displays a password with hash2 encryption in the output screen. However, when using that username, there is no password required. The user can log in to the system by entering their username and then pressing ↵ at the password prompt.

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

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

Default

n/a

Parameters

user-name

the name of the user, up to 32 characters

user-template

Syntax

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

Context

config>system>security

Description

This command configures default security user template parameters.

Parameters

tacplus_default

specifies that the TACACS+ default template is used for the configuration

radius_default

specifies that the RADIUS default template is used for the configuration

access

Syntax

[**no**] **access** [**ftp**] [**snmp**] [**console**] [**scp-sftp**] [**console-port-cli**] [**ssh-cli**] [**telnet-cli**]

[**no**] **access** [**ftp**] [**console**] [**scp-sftp**] [**console-port-cli**] [**ssh-cli**] [**telnet-cli**]

Context

config>system>security>user

config>system>security>user-template

Description

This command specifies user permissions for one or more methods of management access.

If a user requires access to more than one method, multiple methods can be specified in a single command. Multiple commands are treated sequentially.

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

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.

Default

no access

Parameters

ftp

specifies FTP access permission

snmp

specifies SNMP access permission. This keyword is only configurable in the **config>system>security>user** context.

console

specifies SCP/SFTP, Telnet, SSH, and console port CLI access permissions

scp-sftp

specifies SCP/SFTP access permissions

console-port-cli

specifies console port CLI access permission

ssh-cli

specifies SSH CLI access permission

telnet-cli

specifies Telnet CLI access permission

console

Syntax

console

Context

config>system>security>user

config>system>security>user-template

Description

This command enables the context to configure user profile membership for the console.

cannot-change-password

Syntax

[**no**] **cannot-change-password**

Context

config>system>security>user>console

Description

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

To disable a user's privilege to change their password, use the **cannot-change-password** form of the command.

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

local-lockout

Syntax

[**no**] **local-lockout**

Context

config>system>security>user>console

Description

This command prevents console or local serial access if a user is locked out remotely.

The **no** version of this command allows locked-out users to log in only for console or local serial access.

Default

local-lockout

login-exec

Syntax

[**no**] **login-exec** *url-prefix:source-url*

Context

config>system>security>user>console

config>system>security>user-template>console

Description

This command configures a user's login exec file, which executes whenever the user successfully logs in to a console session.

Only one exec file can be configured. If multiple **login-exec** commands are entered for the same user, each subsequent entry overwrites the previous entry.

The **no** form of the command disables the login exec file for the user.

Default

no login exec file is defined

Parameters

url-prefix: source-url

enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that is executed after the user successfully logs in

member

Syntax

member *user-profile-name* [*user-profile-name…*]

no member *user-profile-name*

Context

config>system>security>user>console

Description

This command allows the user access to a profile.

A user can participate in up to eight profiles.

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

Default

default

Parameters

user-profile-name

the user profile name

new-password-at-login

Syntax

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

Context

config>system>security>user>console

Description

This command forces the user to change passwords at the next console or FTP login.

If the user is limited to FTP access, the administrator must create the new password.

The **no** form of the command does not force the user to change passwords.

Default

no new-password-at-login

home-directory

Syntax

home-directory *url-prefix* [*directory*] [*directory/directory…*]

no home-directory

Context

config>system>security>user

config>system>security>user-template

Description

This command configures the local home directory for the user for file access. Files on the 7705 SAR can be accessed locally using the CLI **file** commands and output modifiers, such as > (file redirect), or remotely via FTP or SCP.

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 the command removes the configured home directory.

Default

no 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, root becomes the user's home directory.

Parameters

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

the user's local home directory URL prefix and directory structure, up to 190 characters in length

password

Syntax

password [*password*]

Context

config>system>security>user

Description

This command configures the user password for console and FTP access.

Passwords must be enclosed in double quotes (" ") at the time of password creation if they contain any special characters (such as #, $, or spaces). The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

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

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

The password is stored in an encrypted format in the configuration file when specified.

Parameters

password

the password 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 as follows:

- 56 characters if in unhashed plaintext

  The unhashed plaintext form must meet all the requirements that are defined within the complexity-rules command context.
- 60 characters if hashed with bcrypt
- from 87 to 92 characters if hashed with PBKDF2 SHA-2
- from 131 to 136 characters if hashed with PBKDF2 SHA-3

profile

Syntax

profile *user-profile-name*

no profile

Context

config>system>security>user-template

Description

This command specifies the user profile to associate with the user template. The profile must already be configured with the **profile** command under the **config**>**system**>**security** context.

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

Default

profile "default"

Parameters

user-profile-name

an existing user profile name

public-keys

Syntax

public-keys

Context

config>system>security>user

Description

This command enables the context to configure public keys for SSH.

ecdsa

Syntax

ecdsa

Context

config>system>security>user>public-keys

Description

This command enables the context to configure ECDSA public keys.

ecdsa-key

Syntax

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

no ecdsa-key *key-id*

Context

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

Description

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

Default

n/a

Parameters

key-id

the key identifier

Values 1 to 32

create

keyword required when first creating the ECDSA key. When the key is created, you can navigate into the context without the **create** keyword.

key-value

Syntax

key-value *public-key-value*

no key-value

Context

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

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

Description

This command configures a value for the ECDSA or RSA public key. The public key must be enclosed in quotation marks. For ECDSA, the key is between 1 and 1024 bits. For RSA, the key is between 768 and 4096 bits.

Default

no key-value

Parameters

public-key-value

the value for the ECDSA or RSA key

Values 255 characters max (ECDSA)

800 characters max (RSA)

rsa

Syntax

rsa

Context

config>system>security>user>public-keys

Description

This command enables the context to configure RSA public keys.

rsa-key

Syntax

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

no rsa-key *key-id*

Context

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

Description

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

Parameters

key-id

the key identifier

Values 1 to 32

create

keyword required when first creating the RSA key. When the key is created, you can navigate into the context without the **create** keyword.

restricted-to-home

Syntax

[**no**] **restricted-to-home**

Context

config>system>security>user

config>system>security>user-template

Description

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

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

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

Default

restricted-to-home

Note: This default applies to non-administrative users. For administrative users (**user "admin"**), the default is **no restricted-to-home**.

save-when-restricted

Syntax

[**no**] **save-when-restricted**

Context

config>system>security>user

config>system>security>user-template

Description

This command specifies whether the system allows all configuration save operations (for example, **admin save**) via the CLI even if **restricted-to-home** is enabled.

The home directory does not need to be configured.

The **no** form of the command prevents the user from performing any configuration save operations outside of their home directory when **restricted-to-home** is enabled.

Default

save-when-restricted

snmp

Syntax

snmp

Context

config>system>security>user

Description

This command enables 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 context.

The 7705 SAR always uses the configured SNMPv3 username as the security username.

authentication

Syntax

authentication none

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

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

no authentication

Context

config>system>security>user>snmp

Description

This command configures the SNMPv3 authentication and privacy protocols for the user to communicate with the router. The keys are stored in an encrypted format in the configuration.

The keys configured with these commands must be localized keys, which are a hash of the SNMP engine ID and a password. The password is not entered directly in this command. Use the generate-key command under the **tools>perform>system>management-interface >snmp** context to generate localized authentication and privacy keys. See the 7705 SAR OAM and Diagnostics Guide, "Tools perform commands" for information about this command.

If **authentication none** is configured, only the username is required to allow and authenticate SNMPv3 operations.

The **no** form of the command prevents the username used to configure the command from getting recognized by SNMP, and the same user cannot be used for any SNMP operations.

Default

authentication none – no authentication protocol is configured and privacy cannot be configured

Parameters

none

specifies that no authentication protocol is used

authentication-protocol authentication-key

specifies the SNMPv3 authentication protocol and localized authentication key

Values **hmac-md5-96** – specifies use of the HMAC-MD5-96 authentication protocol; the key must be entered as a 32-character hexadecimal string

hmac-sha1-96 – specifies use of the HMAC-SHA1-96 authentication protocol; the key must be entered as a 40-character hexadecimal string

hmac-sha2-224 – specifies use of the HMAC-SHA2-224 authentication protocol; the key must be entered as a 56-character hexadecimal string

hmac-sha2-256 – specifies use of the HMAC-SHA2-256 authentication protocol; the key must be entered as a 64-character hexadecimal string

hmac-sha2-384 – specifies use of the HMAC-SHA2-384 authentication protocol; the key must be entered as a 96-character hexadecimal string

hmac-sha2-512 – specifies use of the HMAC-SHA2-512 authentication protocol; the key must be entered as a 128-character hexadecimal string

privacy-protocol privacy-key

specifies the SNMPv3 privacy protocol and localized privacy key

Values **cbc-des** – specifies use of the CBC-DES privacy protocol; the key must be entered as a 32-character hexadecimal string. This parameter is not available in FIPS-140-2 mode.

cfb128-aes-128 – specifies use of the CFB128-AES-128 privacy protocol; the key must be entered as a 32-character hexadecimal string

cfb128-aes-192 – specifies use of the CFB128-AES-192 privacy protocol; the key must be entered as a 48-character hexadecimal string

cfb128-aes-256 – specifies use of the CFB128-AES-256 privacy protocol; the key must be entered as a 64-character hexadecimal string

privacy none

specifies that a privacy protocol is not used in the communication

Default privacy none

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 an unencrypted, 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.

group

Syntax

group *group-name*

no group

Context

config>system>security>user>snmp

Description

This command associates (or links) a user to a group name. The access command links the group with one or more views, security models, security levels, and read, write, and notify permissions.

Default

no group name is associated with a user

Parameters

group-name

enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group name per security model.

3.11.2.2.9 CLI script authorization commands

cli-script

Syntax

cli-script

Context

config>system>security

Description

This command enables the context to configure CLI script security.

authorization

Syntax

authorization

Context

config>system>security>cli-script

Description

This command enables the context to authorize CLI script execution for CRON and Event Handling System (EHS) scripts.

cron

Syntax

cron

Context

config>system>security>cli-script>authorization

Description

This command enables the context to configure authorization for the CRON scheduler.

cli-user

Syntax

cli-user *user-name*

no cli-user

Context

config>system>security>cli-script>authorization>cron

config>system>security>cli-script>authorization>event-handler

Description

This command defines the user context under which CRON and EHS CLI scripts must execute in order to authorize the script commands. The user must be a local user; TACACS+ and RADIUS users and authorization are not permitted for **cli-script** authorization.

Two unique users can be defined: one to authorize CLI commands for CRON scripts and one to authorize CLI commands for EHS scripts.

The **no** form of this command configures scripts to execute with no restrictions and without performing authorization.

Default

no cli-user

Parameters

user-name

the name of a user in the local node database. TACACS+ or RADIUS users cannot be used. The user configuration must reference a valid local profile for authorization.

event-handler

Syntax

event-handler

Context

config>system>security>cli-script>authorization

Description

This command enables the context to configure authorization for EHS. EHS is a tool that enables operator-defined behavior to be configured on the 7705 SAR. The operator can define a CLI script that the router executes in response to a log event.

3.11.2.2.10 RADIUS client commands

radius

Syntax

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

Context

config>system>security

Description

This command enables the context to configure RADIUS authentication on the 7705 SAR.

For redundancy, multiple server addresses can be configured for each 7705 SAR.

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

access-algorithm

Syntax

access-algorithm {**direct** | **round-robin**}

[**no**] **access-algorithm**

Context

config>system>security>radius

Description

This command configures the algorithm used to access the set of RADIUS servers. Up to five servers can be configured.

In direct mode, the first server, as defined by the server command, is the primary server. This server is always used first when authenticating a request. In round-robin mode, the server used to authenticate a request is the next server in the list, following the last authentication request. For example, if server 1 is used to authenticate the first request, server 2 is used to authenticate the second request, and so on.

Default

direct

Parameters

direct

first server is always used to authenticate a request

round-robin

server used to authenticate a request is the next server in the list, following the last authentication request

accounting

Syntax

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

Context

config>system>security>radius

Description

This command enables RADIUS accounting. The **no** form of this command disables RADIUS accounting.

Default

no accounting

accounting-port

Syntax

accounting-port *port*

no accounting-port

Context

config>system>security>radius

Description

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

Parameters

port

specifies the UDP port number

Values 1 to 65535

Default 1813

authorization

Syntax

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

Context

config>system>security>radius

Description

This command configures RADIUS authorization parameters for the system.

The **no** form of this command disables RADIUS authorization for the system.

Default

no authorization

port

Syntax

port *port*

no port

Context

config>system>security>radius

Description

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

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

Default

1812 (as specified in RFC 2865, Remote Authentication Dial In User Service (RADIUS))

Parameters

port

the TCP port number to contact the RADIUS server

Values 1 to 65535

retry

Syntax

retry *count*

no retry

Context

config>system>security>radius

Description

This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

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

Default

3

Parameters

count

the retry count

Values 1 to 10

server

Syntax

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

no server *server-index*

Context

config>system>security>radius

Description

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

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

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

Default

no RADIUS servers are configured

Parameters

index

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

Values 1 to 5

ip-address

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

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

ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

key

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

Values up to 20 characters in length

hash

specifies that the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** 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.

timeout

Syntax

timeout *seconds*

no timeout

Context

config>system>security>radius

Description

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

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

Default

3

Parameters

seconds

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

Description

This command specifies whether the user template defined by this entry is to be actively applied to the RADIUS user.

Default

no use-default-template

3.11.2.2.11 TACACS+ client commands

tacplus

Syntax

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

Context

config>system>security

Description

This command enables the context to configure TACACS+ authentication on the 7705 SAR.

For redundancy, multiple server addresses can be configured for each 7705 SAR.

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

accounting

Syntax

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

no accounting

Context

config>system>security>tacplus

Description

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

record-type stop-only

specifies that a stop packet is sent when the command execution is complete

authorization

Syntax

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

Context

config>system>security>tacplus

Description

This command configures TACACS+ authorization parameters for the system.

Default

no authorization

server

Syntax

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

no server index

Context

config>system>security>tacplus

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 the lowest index to the highest index for authentication requests.

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

Default

no TACACS+ servers are configured

Parameters

index

the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.

Values 1 to 5

ip-address

the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

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

key

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

Values up to 128 characters in length

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 an unencrypted, 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.

port

the port ID

Values 0 to 65535

timeout

Syntax

timeout *seconds*

no timeout

Context

config>system>security>tacplus

Description

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

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

Default

3

Parameters

seconds

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

Values 1 to 90

use-default-template

Syntax

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

Context

config>system>security>tacplus

Description

This command specifies whether the user template defined by this entry is to be actively applied to the TACACS+ user.

3.11.2.2.12 802.1x commands

dot1x

Syntax

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

Context

config>system>security

Description

This command enables the context to configure 802.1x network access control on the 7705 SAR.

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

radius-plcy

Syntax

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

Context

config>system>security>dot1x

Description

This command enables the context to configure RADIUS server parameters for 802.1x network access control on the 7705 SAR.

The RADIUS server configured under the **config>system>security>dot1x>radius-plcy** context authenticates clients who get access to the data plane of the 7705 SAR. This configuration differs from the RADIUS server configured under the **config>system>security>radius** context that authenticates CLI login users who get access to the management plane of the 7705 SAR.

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

Parameters

name

the RADIUS policy name, up to 32 characters

create

keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

retry

Syntax

retry *count*

no retry

Context

config>system>security>dot1x

Description

This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

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

Default

3

Parameters

count

the retry count

Values 1 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 *server-index*

Context

config>system>security>dot1x>radius-plcy

Description

This command adds an 802.1x server and configures the IP address, index, and key values.

Up to five 802.1x servers can be configured at any one time. These 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 802.1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

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

Default

n/a

Parameters

server-index

the index for the 802.1x server

Values 1 to 5

ip-address

the IP address of the 802.1x server. Each 802.1x server must have a unique IP address. An error message is generated if the server address is a duplicate.

Values a.b.c.d

key

the secret key to access the 802.1x server. This secret key must match the password on the 802.1x server.

Values up to 20 alphanumeric characters

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 an unencrypted, 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 that involves more variables than the key value alone. This means that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

auth-port

the UDP port number used to contact the RADIUS server for authentication

Values 1 to 65535

acct-port

the UDP port number used to contact the RADIUS server for accounting requests

Values 1 to 65535

server-type

the server type

Values authorization, accounting, or combined

source-address

Syntax

source-address *ip-address*

no source-address

Context

config>system>security>dot1x>radius-plcy

Description

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

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

Default

system IP address

Parameters

ip-address

the source address of the RADIUS packet in dotted-decimal notation

Values 0.0.0.0 to 255.255.255.255

shutdown

Syntax

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

Context

config>system>security>dot1x

config>system>security>dot1x>radius-plcy

Description

This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

The **no** form of the command administratively enables the protocol.

Default

shutdown

timeout

Syntax

timeout *seconds*

no timeout

Context

config>system>security>dot1x>radius-plcy

Description

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

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

Default

5

Parameters

seconds

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

Values 1 to 90

3.11.2.2.13 SSH commands

ssh

Syntax

ssh

Context

config>system>security

Description

This command enables the context to configure the SSH server parameters on the system.

Quitting SSH while in the process of authentication is accomplished by either executing a **ctrl-c** or "~." (tilde and dot), assuming the "~" is the default escape character for the SSH session.

Default

n/a

client-cipher-list

Syntax

client-cipher-list

Context

config>system>security>ssh

Description

This command enables the context to configure the list of allowed ciphers on the SSH client.

Default

n/a

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

Description

This command configures the allowed SSHv2 ciphers that are available on the SSH client or server. Client cipher and server cipher lists are used to negotiate the best compatible cipher between the SSH client and SSH server. Client ciphers are used when the 7705 SAR node is acting as an SSH client; server ciphers are used when the 7705 SAR node is acting as an SSH server.

Each list contains ciphers and their corresponding index values, where a lower index has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest.

The following table lists the default index values used for SSHv2, in order of preference.

Table 11: SSHv2 default index values

Cipher index value	Cipher name
2	aes256-ctr
4	aes192-ctr
6	aes128-ctr
10	aes128-cbc
20	3des-cbc
60	aes192-cbc
70	aes256-cbc

Note: When the 7705 SAR is running in FIPS-140-2 mode, the 3des-cbc cipher is not available.

The **no** form of this command deletes the specified cipher index.

Default

n/a

Parameters

index

the index of the cipher in the list

Values 1 to 255

cipher-name

the allowed cipher name

Values For SSHv2 client ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc

For SSHv2 server ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc

client-kex-list

Syntax

client-kex-list

Context

config>system>security>ssh

Description

This command enables the context to configure a list of preferred KEX algorithms to be used by an SSHv2 client.

Default

n/a

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

Description

This command configures the list of preferred KEX algorithms that are negotiated by the client and server using an SSHv2 phase one handshake.

By default, a KEX client and KEX server each have a hard-coded list that contains the default indexes and their corresponding algorithms. The following table lists the default index values and algorithms, in order of preference.

Table 12: Default KEX index values

KEX index value	KEX algorithm name
200	diffie-hellman-group16-sha512
210	diffie-hellman-group14-sha256
215	diffie-hellman-group14-sha1
220	diffie-hellman-group-exchange-sha1

KEX index value	KEX algorithm name
225	diffie-hellman-group1-sha1

The default list can be changed by manually removing a single index or as many indexes as required using the **no kex** *index* command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required. To go back to using the original hard-coded list, the default KEX indexes must be manually re-entered with their corresponding algorithms.

In a KEX list, the algorithm with the lowest index value has the highest preference in the SSH negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their KEX lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon.

Note: When the 7705 SAR is running in FIPS-140-2 mode, the diffie-hellman-group1-sha1 KEX algorithm is not available.

The **no** form of this command removes the specified KEX index. Removing all the indexes from a client or server list results in an empty list, and any KEX algorithm the client or server brings to the SSHv2 negotiation will be rejected.

Default

no kex

Parameters

index

the index of the KEX algorithm in the list. The list is ordered from highest to lowest.

Values 1 to 255

kex-name

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

client-mac-list

Syntax

client-mac-list

Context

config>system>security>ssh

Description

This command enables the context to configure a list of preferred MAC algorithms to be used by an SSHv2 client.

Default

n/a

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

Description

This command configures the list of preferred MAC algorithms that are negotiated by an SSHv2 server or client.

Each algorithm in the list has a corresponding index value, where a lower index has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest.

The following table lists the default client and server MAC index values used for SSHv2.

Table 13: Default SSHv2 MAC index values

MAC index value	MAC algorithm name
200	hmac-sha2-512
210	hmac-sha2-256
215	hmac-sha1
220	hmac-sha1-96
225	hmac-md5
240	hmac-md5-96

Note: When the 7705 SAR is running in FIPS-140-2 mode, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5, and hmac-mda5-96.

The **no** form of this command removes the specified MAC index from the list.

Default

no mac

Parameters

index

the index of the MAC algorithm in the list

Values 1 to 255

mac-name

the algorithm for calculating the message authentication code

Values hmac-sha2-512, hmac-sha2-256, hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96

key-re-exchange

Syntax

key-re-exchange

Context

config>system>security>ssh

Description

This command enables the context to configure key re-exchange parameters for an SSH client or server.

client

Syntax

client

Context

config>system>security>ssh>key-re-exchange

Description

This command enables the context to configure key re-exchange parameters for an SSH client.

mbytes

Syntax

mbytes {*mbytes*| **disable**}

no mbytes

Context

config>system>security>ssh>key-re-exchange>client

config>system>security>ssh>key-re-exchange>server

Description

This command configures the maximum number of megabytes that can be transmitted during an SSH session before an SSH client or server initiates the key re-exchange procedure.

If both the **mbytes** and **minutes** key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first.

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

Default

1024

Parameters

mbytes

specifies the number of megabytes that can be transmitted during an SSH session before the key re-exchange occurs

Values 1 to 64000

disable

specifies that a session will never time out

minutes

Syntax

minutes {*minutes* | **disable**}

no minutes

Context

config>system>security>ssh>key-re-exchange>client

config>system>security>ssh>key-re-exchange>server

Description

This command configures the maximum time that an SSH session can be up before an SSH client or server initiates the key re-exchange procedure.

If both the **mbytes** and **minutes** key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first.

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

Default

60

Parameters

minutes

specifies the number of minutes before an SSH client or server initiates the key re-exchange

Values 1 to 1440

disable

specifies that a session will never time out

shutdown

Syntax

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

Context

config>system>security>ssh>key-re-exchange>client

config>system>security>ssh>key-re-exchange>server

Description

This command enables or disables initiating of the key re-exchange procedure when the configured thresholds are reached.

Default

no shutdown

server

Syntax

server

Context

config>system>security>ssh>key-re-exchange

Description

This command enables the context to configure key re-exchange parameters for an SSH server.

listening-port

Syntax

listening-port *port*

no listening-port

Context

config>system>security>ssh

Description

This command configures the listening TCP port of the SSH server for incoming SSH connections via base or management routing. VPRN node management is done via GRT leaking and uses base routing.

The **no** form of this command resets the listening port to its default of 22.

Default

no listening port

Parameters

port

specifies the port number

Values 1024 to 49151

preserve-key

Syntax

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

Context

config>system>security>ssh

Description

This command specifies the persistence of the SSH server host key. When enabled, the host key will be saved by the server and restored following a system reboot. This command can only be enabled or disabled when no SSH session is running.

The **no** form of the command specifies that the host key will be held in memory by the SSH server and not be restored following a system reboot.

Default

no preserve-key

server-cipher-list

Syntax

server-cipher-list

Context

config>system>security>ssh

Description

This command enables the context to configure the list of allowed ciphers on the SSH server.

Default

n/a

server-kex-list

Syntax

server-kex-list

Context

config>system>security>ssh

Description

This command enables the context to configure a list of preferred KEX algorithms to be used by an SSHv2 server.

Default

n/a

server-mac-list

Syntax

server-mac-list

Context

config>system>security>ssh

Description

This command enables the context to configure a list of preferred MAC algorithms to be used by an SSHv2 server.

Default

n/a

server-shutdown

Syntax

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

Context

config>system>security>ssh

Description

This command disables the SSH server running on the system. The **no** version of the command enables the SSH server.

When the **no server-shutdown** command is executed, an SSH security key is generated. Unless the **preserve-key** command is enabled, this key is valid until either the node is restarted or the SSH server is stopped with the **server-shutdown** command and restarted. The key size is non-configurable and is set to 2048 for SSHv2 RSA and to 1024 for SSHv2 DSA. Only SSHv2 RSA is supported in FIPS-140-2 mode.

Default

no server-shutdown

3.11.2.2.14 Security TLS commands

tls

Syntax

tls

Context

config>system>security

Description

This command enables the context to configure TLS parameters.

Default

n/a

cert-profile

Syntax

cert-profile *profile-name* **[create]**

no cert-profile *profile-name*

Context

config>system>security>tls

Description

This command creates a new TLS certificate profile or specifies an existing certificate profile. The certificate profile contains the certificates that are sent to the TLS peer to authenticate itself. The TLS server must send this information. The TLS client can optionally send this information upon request from the TLS server.

The **no** form of the command deletes the specified TLS certificate profile.

Default

n/a

Parameters

profile-name

the name of the TLS certificate profile, up to 32 characters in length

create

keyword is mandatory when creating a new certificate profile

entry

Syntax

entry *entry-id* **[create]**

no entry *entry-id*

Context

config>system>security>tls>cert-profile

Description

This command configures an entry for the TLS certificate profile. A certificate profile can have up to eight entries. Currently, TLS uses the entry with the lowest ID number when responding to server requests.

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

Default

n/a

Parameters

entry-id

the identification number of the TLS certificate profile entry

Values 1 to 8

create

keyword is mandatory when creating a new certificate profile

cert

Syntax

cert *cert-filename*

no cert

Context

config>system>security>tls>cert-profile>entry

Description

This command specifies the filename of an imported certificate for the **cert-profile** entry.

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

Default

no cert

Parameters

cert-filename

the filename of the TLS certificate, up to 95 characters in length

key

Syntax

key *key-filename*

no key

Context

config>system>security>tls>cert-profile>entry

Description

This command specifies the filename of an imported key for the **cert-profile** entry.

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

Default

no key

Parameters

key-filename

the filename of the key, up to 95 characters in length

send-chain

Syntax

[no] send-chain

Context

config>system>security>tls>cert-profile>entry

Description

This command enables the sending of certificate authority (CA) certificates and enables the context to configure send-chain information.

By default, the system only sends the TLS client certificate specified by the **cert** command. This command allows the system to send additional CA certificates to the peer. The certificates must be in the chain of certificates specified by the **config>system>security>pki>ca-profile** command. The specification of the send-chain is not necessary for a working TLS profile if the TLS peer has the CA certificate used to sign the client certificate in its own trust anchor.

For example, with a TLS client running on the 7705 SAR, the ROOT CA certificate resides on the TLS server, but the subsequent SUB-CA certificate needed to complete the chain resides within the 7705 SAR. The **send-chain** command allows these SUB-CA certificates to be sent from the 7705 SAR to the peer to be authenticated using the ROOT CA certificate that resides on the peer.

The **no** form of the command disables the send-chain.

Default

no send-chain

ca-profile

Syntax

[no] ca-profile *name*

Context

config>system>security>tls>cert-profile>entry>send-chain

Description

This command specifies that a CA certificate in the specified **ca-profile** is to be sent to the peer.

Up to seven configurations of this command are allowed in the same entry.

The **no** form of the command disables the transmission of a CA certificate from the specified CA profile.

Default

n/a

Parameters

name

the name of an existing CA

shutdown

Syntax

[no] shutdown

Context

config>system>security>tls>cert-profile

Description

This command disables the certificate profile. When the certificate profile is disabled, it will not be sent to the TLS server.

The **no** form of the command enables the certificate profile and allows it to be sent to the TLS server.

Default

shutdown

client-cipher-list

Syntax

client-cipher-list *name* **[create]**

no client-cipher-list *name*

Context

config>system>security>tls

Description

This command creates a cipher list or specifies an existing list that the client sends to the server in the client Hello message. The list contains ciphers that are supported and preferred by the 7705 SAR to be used in the TLS session. The server matches this list against the server cipher list. The most preferred cipher found in both lists is chosen.

The **no** form of the command deletes the specified cipher list.

Default

n/a

Parameters

name

the name of the client cipher list, up to 32 characters in length

create

keyword is mandatory when creating a new certificate profile

cipher

Syntax

cipher *index* **name** *cipher-suite-code*

no cipher *index*

Context

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

Description

This command configures the TLS cipher suite code to be negotiated by the server and client.

The **no** form of the command removes the cipher suite code.

Default

n/a

Parameters

index

the index number of the cipher suite code, which indicates the position of the code in the negotiation list (the lower the index number, the higher the priority of the code)

Values 1 to 255

cipher-suite-code

specifies the cipher suite code

Values tls-rsa-with3des-ede-cbc-sha | tls-rsa-with-aes128-cbc-sha | tls-rsa-with-aes256-cbc-sha | tls-rsa-with-aes128-cbc-sha256 | tls-rsa-with-aes256-cbc-sha256

tls13-cipher

Syntax

tls13-cipher *index* **name** *cipher-suite-code*

no tls13-cipher *index*

Context

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

Description

This command configures the TLS 1.3 supported ciphers that are used by the client and server.

The **no** form of the command removes the cipher suite code.

Default

n/a

Parameters

index

the index number of the TLS 1.3 cipher suite code, which indicates the position of the code in the negotiation list (the lower the index number, the higher the priority of the code)

Values 1 to 255

cipher-suite-code

specifies the cipher suite code

Values tls-aes128-gcm-sha256 | tls-aes256-gcm-sha384 | tls-chacha20-poly1305-sha256 (not supported in FIPS mode) | tls-aes128-ccm-sha256 | tls-aes128-ccm8-sha256

client-group-list

Syntax

client-group-list *name* **[create]**

no client-group-list *name*

Context

config>system>security>tls

Description

This command creates a client group list or specifies an existing group list that the client sends in a client Hello message. The list contains group suite codes configured with the **tls13-group** command.

The **no** form of the command removes the client group list.

Default

n/a

Parameters

name

the name of the client group list, up to 32 characters

create

keyword is mandatory when creating a new certificate profile

tls13-group

Syntax

tls13-group *index* **name** *group-suite-code*

no tls13-group *index*

Context

config>system>security>tls>client-group-list

Description

This command configures the TLS 1.3 supported group suite codes sent by the client in the Hello message.

The 7705 SAR supports the use of Elliptic-curve Diffie-Hellman Ephemeral (ECDHE) groups.

The **no** form of the command removes the group suite code.

Default

n/a

Parameters

index

the index number of the group suite code, which indicates the position of the code in the negotiation list (the lower the index number, the higher the priority of the code)

Values 1 to 255

group-suite-code

specifies the group suite code

Values tls-ecdhe-256 | tls-ecdhe-384 | tls-ecdhe-521 | tls-x25519 | tls-x448

client-signature-list

Syntax

client-signature-list *name* **[create]**

no client-signature-list *name*

Context

config>system>security>tls

Description

This command creates a client signature list or specifies an existing signature list that the client sends in a client Hello message.

The **no** form of the command removes the client signature list.

Default

n/a

Parameters

name

the name of the client signature list, up to 32 characters

create

keyword is mandatory when creating a new certificate profile

tls13-signature

Syntax

tls13-signature *index* **name** *signature-suite-code*

no tls13-signature *index*

Context

config>system>security>tls>client-signature-list

Description

This command configures the TLS 1.3 supported signature suite codes sent in the client Hello message.

The **no** form of the command removes the signature suite code.

Default

n/a

Parameters

index

the index number of the TLS 1.3 signature suite code, which indicates the position of the code in the negotiation list (the lower the index number, the higher the priority of the code)

Values 1 to 255

signature-suite-code

specifies the signature suite code

Values tls-rsa-pkcs1-sha256 | tls-rsa-pkcs1-sha384 | tls-rsa-pkcs1-sha512 | tls-ecdsa-secp256r1-sha256 | tls-ecdsa-secp384r1-sha384 | tls-ecdsa-secp521r1-sha512 | tls-rsa-pss-rsae-sha256 | tls-rsa-pss-rsae-sha384 | tls-rsa-pss-rsae-sha512 | tls-rsa-pss-pss-sha256 | tls-rsa-pss-pss-sha384 | tls-rsa-pss-pss-sha512 | tls-ed25519 | tls-ed448

client-tls-profile

Syntax

client-tls-profile *name* **[create]**

no client-tls-profile *name*

Context

config>system>security>tls

Description

This command creates a TLS client profile or specifies an existing client profile to be assigned to applications for encryption. Up to 16 TLS client profiles can be configured.

The **no** form of the command deletes the TLS client profile.

Default

n/a

Parameters

name

the name of the TLS client profile, up to 32 characters in length

create

keyword is mandatory when creating a new certificate profile

cert-profile

Syntax

cert-profile *name*

no cert-profile

Context

config>system>security>tls>client-tls-profile

Description

This command assigns an existing TLS certificate profile to be used by the TLS client profile. This certificate is sent to the server for authentication of the client and public key.

The **no** form of the command removes the TLS certificate profile assignment.

Default

no cert-profile

Parameters

name

the name of the TLS certificate profile

cipher-list

Syntax

cipher-list *name*

no cipher-list

Context

config>system>security>tls>client-tls-profile

Description

This command assigns an existing cipher list to be used by the TLS client profile for negotiation in the client Hello message.

Default

no cipher-list

Parameters

name

the name of the cipher list

group-list

Syntax

group-list *name*

no group-list

Context

config>system>security>tls>client-tls-profile

Description

This command assigns an existing TLS 1.3 group list to the TLS client profile.

The **no** form of the command removes the group list from the client profile.

Default

no group-list

Parameters

name

the name of the group list

protocol-version

Syntax

protocol-version *TLS version*

no protocol-version

Context

config>system>security>tls>client-tls-profile

Description

This command configures the TLS version to be negotiated between the client and server.

When configured, the client adds the specified version as a supported version in its Hello message to the server. If **tls-version-all** is specified, the client adds both TLS 1.2 and TLS 1.3 as supported versions in its Hello message.

The **no** form of the command reverts to the default TLS version.

Default

tls-version12

Parameters

TLS version

specifies the TLS version to include in the client Hello message

Values tls-version12 | tls-version13 | tls-version-all

shutdown

Syntax

[no] shutdown

Context

config>system>security>tls>client-tls-profile

Description

This command disables the client TLS profile.

The **no** form of the command enables the client TLS profile.

Default

shutdown

signature-list

Syntax

signature-list *name*

no signature-list

Context

config>system>security>tls>client-tls-profile

Description

This command assigns an existing TLS 1.3 signature list to the TLS client profile.

The **no** form of the command removes the signature list from the client profile.

Default

no signature-list

Parameters

name

the name of the signature list

trust-anchor-profile

Syntax

trust-anchor-profile *name*

no trust-anchor-profile

Context

config>system>security>tls>client-tls-profile

Description

This command assigns an existing trust anchor profile to be used by this TLS client profile to authenticate the server.

The **no** form of the command removes the trust anchor profile from the client profile.

Default

no trust-anchor-profile

Parameters

name

the name of the trust anchor profile

trust-anchor-profile

Syntax

trust-anchor-profile *name* **[create]**

no trust-anchor-profile *name*

Context

config>system>security>tls

Description

This command creates a trust anchor profile or specifies an existing trust anchor profile to be used in the TLS client profile. The trust anchor is used for authentication of the server certificate. Up to 16 trust anchor profiles can be configured, with up to 8 trust anchors in each profile.

Default

n/a

Parameters

name

the name of the trust anchor profile, up to 32 characters

create

keyword is mandatory when creating a new certificate profile

trust-anchor

Syntax

[no] trust-anchor *ca-profile-name*

Context

config>system>security>tls>trust-anchor-profile

Description

This command configures a trust anchor with a CA profile used by the TLS profile. Up to eight trust anchors can be configured under the TLS profile.

Default

n/a

Parameters

ca-profile-name

the name of the TLS trust anchor

3.11.2.2.15 Keychain authentication commands

keychain

Syntax

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

Context

config>system>security

Description

This command enables the context to configure keychain parameters that are used to authenticate protocol communications. A keychain must be configured on the system before it can be applied to a protocol session.

The keychain must include at least one key entry to be valid.

The **no** form of the command removes the keychain and all commands configured in the keychain context. If the keychain is associated with a protocol when the **no keychain** command is entered, the command will be rejected and an error indicating that the keychain is in use will be displayed.

Default

n/a

Parameters

keychain-name

the keychain name, up to 32 characters

direction

Syntax

direction

Context

config>system>security>keychain

Description

This command specifies the stream direction on which the keys will be applied.

Default

n/a

bi

Syntax

bi

Context

config>system>security>keychain>direction

Description

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

Default

n/a

entry

Syntax

entry *entry-id* [**key** *authentication-key* | *hash-key* | *hash2-key* [**hash** | **hash2**] **algorithm** *algorithm*]

no entry *entry-id*

Context

config>system>security>keychain>direction>bi

config>system>security>keychain>direction>uni>receive

config>system>security>keychain>direction>uni>send

Description

This command defines a key in the keychain. A keychain must have at least one key entry to be valid.

The **key** and **algorithm** keywords are mandatory when the entry is first created.

The **no** form of the command removes the entry from the keychain. If the key is the active key for sending, this command will cause a new active key to be selected (if one is available). If the key is the only possible send key, the command will be rejected and an error indicating that the configured key is the only available send key will be displayed. If the key is one of the eligible keys for receiving, it will be removed. If the key is the only eligible key for receiving, the command will be rejected and an error indicating that this is the only eligible key will be displayed.

Default

n/a

Parameters

entry-id

the ID of the key entry

Values 0 to 63 | null-key (the **null-key** parameter does not apply and should be ignored)

key

the authentication key ID that is used along with *keychain-name* and **direction** to uniquely identify this particular key entry

authentication-key

the authentication key that will be used by the encryption algorithm, up to 20 characters in any combination of letters and numbers. The key is used to sign and authenticate a protocol packet.

Values the 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 is configured with fewer than this number of bits, it is padded internally with zero bits up to the correct length.

hash-key | *hash2-key*

the hash key. The key can be any combination of ASCII characters up to 33 for the *hash-key* and up to 96 for the *hash2-key* (encrypted). If spaces are used in the string, the entire string must be enclosed in double quotes.

This parameter 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** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2

specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

algorithm

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 for TCP authentication (BGP and LDP)

hmac-sha-1-96 – specifies an algorithm based on SHA-1 for OSPF, RSVP-TE, and TCP authentication

password – specifies a simple password authentication for OSPF and IS-IS

message-digest – specifies the MD5 hash authentication for OSPF

hmac-sha-1 – specifies the SHA-1 algorithm for OSPF, IS-IS, and RSVP-TE authentication

hmac-sha-256 – specifies the SHA-256 algorithm for OSPF, IS-IS, and RSVP-TE authentication

hmac-md5 – specifies the MD5 hash authentication for IS-IS and RSVP-TE

begin-time

Syntax

begin-time *date hours-minutes* [**UTC**]

begin-time {**now** | **forever**}

no begin-time

Context

config>system>security>keychain>direction>bi>entry

config>system>security>keychain>direction>uni>receive>entry

config>system>security>keychain>direction>uni>send>entry

Description

This command specifies the calendar date and time after which the key specified by the keychain authentication key entry is used to sign and authenticate the protocol stream.

Each entry within a bidirectional keychain or for a keychain direction (if unidirectional keys are used) must have a unique begin time.

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.

Default

forever

Parameters

date hours-minutes

the date (in YYYY/MM/DD format) and time (in hh:mm[:ss] format) at which the key becomes active

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 (current system time)

forever

specifies that the key is always inactive

option

Syntax

option {**basic** | **isis-enhanced**}

no option

Context

config>system>security>keychain>direction>bi>entry

Description

This command enables options to be associated with the authentication key for IS-IS. The command is only applicable for IS-IS and will be ignored by other protocols associated with the keychain.

Default

no option

Parameters

basic

specifies that IS-IS should use RFC 5304 encoding of the authentication information

isis-enhanced

specifies that IS-IS should use RFC 5310 encoding of the authentication information

tolerance

Syntax

tolerance {*seconds* | **forever**}

no tolerance

Context

config>system>security>keychain>direction>bi>entry

config>system>security>keychain>direction>uni>receive>entry

Description

This command configures the amount of time that an eligible receive key overlaps with the currently active key. During that time, packets with either key will be accepted. Tolerance only applies to received packets. Transmitted packets always use the newest key, regardless of the tolerance value.

If a tolerance value is set for a key, the key is returned as part of the key set if the current time is within the key's begin time, plus or minus the tolerance value. For example, if the begin time is 12:00 p.m. and the tolerance is 600 seconds, the new key should be included from 11:55 a.m. and the key to be replaced should be included until 12:05 p.m.

Default

300

Parameters

seconds

specifies the length of time that an eligible receive key overlaps with the active key

Values 0 to 4294967294 seconds

forever

specifies that an eligible receive key will overlap with the active key forever

uni

Syntax

uni

Context

config>system>security>keychain>direction

Description

This command configures keys for send or receive stream directions.

Default

n/a

receive

Syntax

receive

Context

config>system>security>keychain>direction>uni

Description

This command enables the receive context. Entries defined under this context are used to authenticate packets that are received by the router.

Default

n/a

end-time

Syntax

end-time *date hours-minutes* [**UTC**]

end-time {**now** | **forever**}

no end-time

Context

config>system>security>keychain>direction>uni>receive>entry

Description

This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to authenticate the protocol stream.

Default

forever

Parameters

date hours minutes

the date (in YYYY/MM/DD format) and time (in hh:mm[:ss] format) after which the key is no longer eligible to sign and authenticate the protocol stream. If no year is specified, the system assumes the current year.

UTC

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

now

specifies that the key should become inactive immediately (current system time)

forever

specifies that the key is always active

send

Syntax

send

Context

config>system>security>keychain>direction>uni

Description

This command enables the send context. Entries defined under this context are used to sign packets that are being sent by the router to another device.

Default

n/a

tcp-option-number

Syntax

tcp-option-number

Context

config>system>security>keychain

Description

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

receive

Syntax

receive *option-number*

no receive

Context

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

Description

This command configures the TCP option number that will be accepted in the header of received TCP packets.

Default

254

Parameters

option-number

the TCP option number to be used in the TCP header

Values 253, 254, 253&254

send

Syntax

send *option-number*

no send

Context

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

Description

This command configures the TCP option number that will be inserted in the header of sent TCP packets.

Default

254

Parameters

option-number

the TCP option number to be used in the TCP header

Values 253, 254

3.11.2.2.16 Login control commands

login-control

Syntax

login-control

Context

config>system

Description

This command enables the context to configure the session control for console, FTP, SSH, and Telnet sessions.

exponential-backoff

Syntax

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

Context

config>system>login-control

Description

This command enables the exponential backoff of the login prompt. The **exponential-backoff** command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try **admin** with any conceivable password.

The **no** form of the command disables exponential-backoff.

Default

no exponential-backoff

ftp

Syntax

ftp

Context

config>system>login-control

Description

This command enables the context to configure FTP login control parameters.

inbound-max-sessions

Syntax

inbound-max-sessions *value*

no inbound-max-sessions

Context

config>system>login-control>ftp

Description

This command configures the maximum number of concurrent inbound FTP sessions.

This value is the combined total of inbound and outbound sessions.

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

Default

3

Parameters

value

the maximum number of concurrent FTP sessions on the node

Values 0 to 5

idle-timeout

Syntax

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

no idle-timeout

Context

config>system>login-control

Description

This command configures the idle timeout for FTP, console, SSH, and Telnet sessions before the session is terminated by the system.

By default, each idle FTP, console, SSH, or Telnet session times out after 30 minutes of inactivity.

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

Default

30

Parameters

minutes

the idle timeout in minutes

Values 1 to 1440

disable

when the **disable** option is specified, a session will never time out. To re-enable idle timeout, enter the command without the **disable** option.

login-banner

Syntax

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

Context

config>system>login-control

Description

This command enables or disables the display of a login banner. The login banner contains the 7705 SAR copyright and build date information for a console login attempt.

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

motd

Syntax

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

no motd

Context

config>system>login-control

Description

This command creates the message of the day that is displayed after a successful console login. Only one message can be configured.

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

Default

no motd

Parameters

url-prefix: source-url

when the message of the day is present as a text file, provide both the *url-prefix* and the *source-url* of the file containing the message of the day. The URL prefix can be local or remote.

motd-text-string

the text of the message of the day, up to 900 characters long. 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.

pre-login-message

Syntax

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

no pre-login-message

Context

config>system>login-control

Description

This command creates a message displayed prior to console login attempts on the console via Telnet.

Only one message can be configured. If multiple pre-login messages are configured, the last message entered overwrites the previous entry.

The system name can be added to an existing message without affecting the current pre-login message.

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

Default

no pre-login-message

Parameters

login-text-string

a text string, up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

name

when the keyword **name** is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.

ssh

Syntax

ssh

Context

config>system>login-control

Description

This command enables the context to configure SSH login control parameters.

disable-graceful-shutdown

Syntax

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

Context

config>system>login-control>ssh

Description

This command disables graceful shutdown of SSH sessions.

By default, SSH always performs a graceful shutdown on a TCP connection. When graceful shutdown is disabled, SSH sends a FIN message and then immediately terminates the connection.

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

Default

no disable-graceful-shutdown

inbound-max-sessions

Syntax

inbound-max-sessions *value*

no inbound-max-sessions

Context

config>system>login-control>ssh

Description

This command limits the number of inbound SSH sessions (channels). Each 7705 SAR router is limited to a total of 15 inbound SSH sessions (IPv4 and IPv6).

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

Default

5

Parameters

value

the maximum number of concurrent inbound SSH sessions, expressed as an integer

Values 0 to 15

outbound-max-sessions

Syntax

outbound-max-sessions *value*

no outbound-max-sessions

Context

config>system>login-control>ssh

Description

This command limits the number of outbound SSH sessions (channels). Each 7705 SAR router is limited to a total of 15 outbound SSH sessions (IPv4 and IPv6).

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

Default

5

Parameters

value

the maximum number of concurrent outbound SSH sessions, expressed as an integer

Values 0 to 15

telnet

Syntax

telnet

Context

config>system>login-control

Description

This command enables the context to configure the Telnet login control parameters.

enable-graceful-shutdown

Syntax

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

Context

config>system>login-control>telnet

Description

This command enables graceful shutdown of Telnet sessions.

When graceful shutdown is enabled, Telnet sends a FIN message and waits for an acknowledgment before terminating the TCP connection.

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

Default

no enable-graceful-shutdown

inbound-max-sessions

Syntax

inbound-max-sessions *value*

no inbound-max-sessions

Context

config>system>login-control>telnet

Description

This command limits the number of inbound Telnet sessions. Each 7705 SAR router is limited to a total of 15 inbound Telnet sessions (IPv4 and IPv6).

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

Default

5

Parameters

value

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

Values 0 to 15

outbound-max-sessions

Syntax

outbound-max-sessions *value*

no outbound-max-sessions

Context

config>system>login-control>telnet

Description

This command limits the number of outbound Telnet sessions. Each 7705 SAR router is limited to a total of 15 outbound Telnet sessions (IPv4 and IPv6).

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

Default

5

Parameters

value

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

Values 0 to 15

ttl-security

Syntax

ttl-security *min-ttl-value*

no ttl-security

Context

config>system>login-control>telnet

config>system>login-control>ssh

Description

This command configures TTL security parameters for incoming packets. When the feature is enabled, SSH or Telnet connections will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer.

The **no** form of the command disables TTL security.

Default

no ttl-security

Parameters

min-ttl-value

specifies the minimum TTL value for an incoming packet

Values 1 to 255

3.11.2.3 Show commands

- Security show commands
- Login control show commands

3.11.2.3.1 Security show commands

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

access-group

Syntax

access-group [*group-name*]

Context

show>system>security

Description

This command displays SNMP access group information.

Parameters

group-name

displays information for the specified access group

Output

The following output is an example of system security access group information, and Table 14: System security access group field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-7#
```

Table 14: System security access group field descriptions

Label	Description
Group name	The access group name
Security model	The security model required to access the views configured in this node
Security level	Specifies the required authentication and privacy levels to access the views configured in this node

Label	Description
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

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 security authentication information, and Table 15: System security authentication field descriptions describes the fields.

Output example

```
A:ALU-4# show system security authentication
===============================================================================
Authentication                  sequence : radius tacplus local
===============================================================================
type                                status  timeout      retry
   server address                           (secs)       count
-------------------------------------------------------------------------------
radius
   10.10.10.103                     up       5             5
radius
   10.10.0.1                        up       5             5
radius
   10.10.0.2                        up       5             5
tacplus
   10.10.0.9(49)                    down     5            n/a
-------------------------------------------------------------------------------
radius admin status  : up
tacplus admin status : down
health check         : enabled (interval 30)
-------------------------------------------------------------------------------
No. of Servers: 4
===============================================================================
```

```
A:ALU-4#
```

```
A:ALU-7>show>system>security# authentication statistics
===============================================================================
Authentication                  sequence : radius tacplus local
===============================================================================
type                               status  timeout        retry
   server address                          (secs)         count
-------------------------------------------------------------------------------
radius
   10.10.10.103                    up        5             5
radius
   10.10.0.1                       up        5             5
radius
   10.10.0.2                       up        5             5
tacplus
   10.10.0.9(49)                   down      5            n/a
-------------------------------------------------------------------------------
radius admin status  : up
tacplus admin status : down
health check         : enabled (interval 30)
-------------------------------------------------------------------------------
No. of Servers: 4
===============================================================================
Login Statistics
===============================================================================
server address                                          conn    accepted   rejected
                                                        errors  logins     logins
-------------------------------------------------------------------------------
10.10.10.103                                            0       0          0
10.10.0.1                                               0       0          0
10.10.0.2                                               0       0          0
10.10.0.9                                               0       0          0
local                                                   n/a     1          0
===============================================================================
Authorization Statistics (TACACS+)
===============================================================================
server address                                          conn    sent       rejected
                                                        errors  pkts       pkts
-------------------------------------------------------------------------------
10.10.0.9                                               0       0          0
===============================================================================
Accounting Statistics
===============================================================================
server address                                          conn    sent       rejected
                                                        errors  pkts       pkts
-------------------------------------------------------------------------------
10.10.10.103                                            0       0          0
10.10.0.1                                               0       0          0
10.10.0.2                                               0       0          0
===============================================================================
A:ALU-7#
```

Table 15: System security authentication field descriptions

Label	Description
Sequence	The sequence in which authentication is processed
Server address	The IP address of the RADIUS server

Label	Description
Status	The current status of the RADIUS server
Type	The authentication type
Timeout (secs)	The number of seconds the router waits for a response from a RADIUS server
Retry count	The number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server
Connection errors	The number of times a user has attempted to log in irrespective of whether the login succeeded or failed
Accepted logins	The number of times the user has successfully logged in
Rejected logins	The number of unsuccessful login attempts
Sent packets	The number of packets sent
Rejected packets	The number of packets rejected

communities

Syntax

communities

Context

show>system>security

Description

This command displays SNMP communities and characteristics.

Output

The following output is an example of community information, and Table 16: Communities field descriptions describes the fields.

Output example

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

```
No. of Communities: 3
===============================================================================
A:ALU-48#
```

Table 16: Communities field descriptions

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

cpm-filter

Syntax

cpm-filter ip-filter [**entry** *entry-id*]

cpm-filter ipv6-filter [**entry** *entry-id*]

Context

show>system>security

Description

This command displays information for CPM (CSM) filters.

If an entry number is not specified, all entries are displayed.

Parameters

entry-id

displays information for the specified CPM filter entry

Values 1 to 9999

Default all filter entries

Output

The following output is an example of CPM filter information, and Table 17: CPM filter field descriptions describes the fields.

Output example

```
A:ALU-35# show system security cpm-filter ip-filter
===============================================================================
CPM IP Filters
===============================================================================
Entry-Id  Dropped   Forwarded Description
-------------------------------------------------------------------------------
2         0         0         CPM filter #2
3         25880     0         CPM filter #3
4         25880     0         CPM filter #4
5         25882     0         CPM filter #5
6         25926     0         CPM filter #6
7         25926     0         CPM filter #7
8         25944     0         CPM filter #8
9         25950     0         CPM filter #9
10        25968     0         CPM filter #10
11        25984     0         CPM filter #11
12        26000     0         CPM filter #12
13        26018     0         CPM filter #13
14        26034     0         CPM filter #14
15        26050     0         CPM filter #15
===============================================================================
A:ALU-35#
```

```
A:ALU-35# show system security cpm-filter ip-filter entry 2
===============================================================================
CPM IP Filter Entry
===============================================================================
Entry Id           : 2
Description : CPM filter #2
-------------------------------------------------------------------------------
Filter Entry Match Criteria :
-------------------------------------------------------------------------------
Log Id             : 101
Src. IP            : 10.4.101.2/32      Src. Port          : 0
Dest. IP           : 10.4.101.1/32      Dest. Port         : 0
Protocol           : tcp                Dscp               : ef
ICMP Type          : Undefined          ICMP Code          : Undefined
Fragment           : True               Option-present     : Off
IP-Option          : n/a                Multiple Option    : True
TCP-syn            : Off                TCP-ack            : True
Match action       : Drop
Dropped pkts       : 0                  Forwarded pkts     : 0
===============================================================================
A:ALU-35#
```

```
A:ALU-35# show system security cpm-filter ipv6-filter entry 101
===============================================================================
CPM IPv6 Filter Entry
===============================================================================
Entry Id : 1
Description : CPM-Filter 11::101:2 #101
-------------------------------------------------------------------------------
Filter Entry Match Criteria :
-------------------------------------------------------------------------------
Log Id : n/a
```

```
Src. IP : 11::101:2       Src. Port : 0
Dest. IP : 11::101:1      Dest. Port : 0
next-header : none Dscp : Undefined
ICMP Type : Undefined     ICMP Code : Undefined
TCP-syn : Off             TCP-ack : Off
Match action : Drop
Dropped pkts : 25880      Forwarded pkts : 0
===============================================================================
```

Table 17: CPM filter field descriptions

Label	Description
CPM IP (or IPv6) Filter Entry	
Entry-id	Displays information for the specified CPM filter entry
Dropped	The number of dropped events
Forwarded	The number of forwarded events
Description	The CPM filter description
Filter Entry Match Criteria	
Log Id	The log ID where matched packets will be logged
Src. IP	The source IP address
Dest. IP	The destination IP address
Protocol	The Protocol field in the IP header (IPv4 filters only)
next-header	The next header ID. Undefined indicates no next header is specified. (IPv6 filters only)
ICMP Type	The ICMP type field in the ICMP header
Fragment	The 3-bit fragment flags or 13-bit fragment offset field (IPv4 filters only)
IP-Option	The IP option setting (IPv4 filters only)
TCP-syn	The SYN flag in the TCP header
Match action	When the criteria matches, displays drop or forward packet
Dropped pkts	The number of matched dropped packets
Src. Port	The source port number (range)
Dest. Port	The destination port number (range)
Dscp	The DSCP field in the IP header
ICMP Code	The ICMP code field in the ICMP header

Label	Description
Option-present	The option present setting (IPv4 filters only)
Multiple Option	The multiple option setting (IPv4 filters only)
TCP-ack	The ACK flag in the TCP header
Match action	When the criteria matches, displays drop or forward packet
Next Hop	If match action is forward, indicates destination of the matched packet
Forwarded pkts	Indicates number of matched forwarded packets

keychain

Syntax

keychain [*keychain*] [**detail**]

Context

show>system>security

Description

This command displays information about keychains.

If a keychain name is not specified, all keychains are displayed.

Parameters

keychain

displays information for the specified keychain

detail

displays detailed keychain information

Output

The following output is an example of keychain information, and Table 18: Keychain field descriptions describes the fields.

Output example

```
===============================================================================
Key chain:ospf-md5
===============================================================================
Description                : MD5 keychain for OSPF interfaces
TCP-Option number send     : 254                    Admin state   : Up
TCP-Option number receive  : 254                    Oper state    : Up
Used by                    : None
Expired                    : No
===============================================================================
```

```
*A:ALU-35#
```

```
A:ALU-35# show system security keychain ospf-md5 detail
===============================================================================
Key entries for key chain: ospf-md5
===============================================================================
Id               : 0                    Direction        : send-receive
Algorithm        : message-digest       Option           : none
Admin State      : Up                   RX Valid         : No
TX Active        : No                   Tolerance        : 300
Begin Time       : 2016/06/01 01:01:00  Begin Time (UTC) : 2016/06/01 01:01:00
End Time         : 2016/09/01 01:01:00  End Time (UTC)   : 2016/09/01 01:01:00
===============================================================================
Id               : 1                    Direction        : send-receive
Algorithm        : message-digest       Option           : none
Admin State      : Up                   RX Valid         : Yes
TX Active        : Yes                  Tolerance        : 600
Begin Time       : 2016/09/01 01:01:00  Begin Time (UTC) : 2016/09/01 01:01:00
End Time         : Forever              End Time (UTC)   : Forever
===============================================================================
*A:Sar18 Dut-B#
```

Table 18: Keychain field descriptions

Label	Description
Key chain: *name*	
Description	The text string description for the keychain
TCP-Option number send	The TCP option number to be inserted in the header of sent TCP packets
Admin state	The administrative state of the keychain: up or down
TCP-Option number receive	The TCP option number that will be accepted in the header of received TCP packets
Oper state	The operational state of the keychain: up or down
Used by	The protocols associated with this keychain
Expired	Indicates whether the keychain has expired
Key entries for key chain: *name*	
Id	The ID of the key entry
Direction	The stream direction on which keys will be applied for this entry: send, receive, or send-receive
Algorithm	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	The administrative state of the key entry: up or down

Label	Description
RX Valid	Indicates if the receive key is valid
TX Active	Indicates if the transmit (sent) key is active
Tolerance	The tolerance time configured for support of both currently active and new keys
Begin Time	The time at which the new key is used to sign and/or authenticate protocol packets
Begin Time (UTC)	The begin time in UTC time
End Time	The time at which the key is no longer eligible to authenticate protocol packets
End Time (UTC)	The end time in UTC time

management-access-filter

Syntax

management-access-filter ip-filter [**entry** *entry-id*]

management-access-filter ipv6-filter [**entry** *entry-id*]

Context

show>system>security

Description

This command displays management access control filter information.

If no specific entry number is specified, all entries are displayed.

Parameters

entry-id

displays information for the specified management access filter entry

Values 1 to 9999

Default All filter entries

Output

The following output is an example of management access filter information, and Table 19: Management access filter field descriptions describes the fields.

Output example

```
A:ALU-7# show system security management-access-filter ip-filter entry 1
```

```
===============================================================================
IPv4 Management Access Filters
===============================================================================

filter type:  : ip
Def. Action   : permit
Admin Status  : enabled (no shutdown)
-------------------------------------------------------------------------------
Entry         : 1
Description   : test description
Src IP        : 10.10.10.104
Src interface : undefined
Dest port     : 10.10.10.103
Protocol      : 6
Router        : undefined
Action        : permit
Log           : disabled
Matches       : 0
===============================================================================
A:ALU-7#
```

```
A:ALU-7# show system security management-access-filter ipv6-filter entry 2
===============================================================================
IPv6 Management Access Filter
===============================================================================
filter type   : ipv6
Def. Action   : permit
Admin Status  : enabled (no shutdown)
-------------------------------------------------------------------------------
Entry         : 1
Src IP        : 2001::1/128
Flow label    : undefined
Src interface : undefined
Dest port     : undefined
Next-header   : undefined
Router        : undefined
Action        : permit
Log           : enabled
Matches       : 0
===============================================================================
A:ALU-7#
```

Table 19: Management access filter field descriptions

Label	Description
IPv4 (or IPv6) Management Access Filters	
filter type	The management access filter type
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

Label	Description
Admin Status	Up: indicates that the management access filter is administratively enabled
	Down: indicates that the management access filter is administratively disabled
Entry	The entry ID in a policy or filter table
Description	A text string describing the filter
Src IP	The source IP address used for management access filter match criteria
Flow label	The flow label to match (IPv6 filters only)
Src interface	The interface name for the next hop to which the packet should be forwarded if it hits this filter entry
Dest port	The destination port
Next-header	The next header ID to match. Undefined indicates no next header is specified. (IPv6 filters only)
Protocol	The IP protocol to match (IPv4 filters only)
Action	The action to take for packets that match this filter entry
Matches	The number of times a management packet has matched this filter entry

password-options

Syntax

password-options

Context

show>system>security

Description

This command displays configured password options.

Output

The following output is an example of password options information, and Table 20: Password options field descriptions describes the fields.

Output example

```
A:7705:Dut-A# show system security password-options
```

```
===============================================================================
Password Options
===============================================================================
Password aging in days                          : none
Time required between password changes          : 0d 00:10:00
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
User password history length                    : disabled
Password hashing                                : bcrypt
Accepted password length                        : 6..56 characters
Credits for each character class                : none
Number of required characters per class         : none
Minimum number of required character classes    : 0
Required distance with previous password        : 5
Allow consecutively repeating a character       : always
Allow passwords containing username             : no
Palindrome allowed                              : no
===============================================================================
A:7705:Dut-A#
```

Table 20: Password options field descriptions

Label	Description
Password aging in days	The number of days a user password is valid before the user must change their password
Time required between password changes	The time interval required before a password can be changed
Number of invalid attempts permitted per login	The number of unsuccessful login attempts allowed for the specified time
Time in minutes per login attempt	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)	The lockout period, in minutes, during which the user is not allowed to log in
Authentication order	The sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords
User password history length	The number of recent passwords stored in the history file to compare against new passwords. If a new password matches any of the passwords in the history file, it is rejected
Password hashing	The password hashing type, either bcrypt, sha2-pbkdf2, or sha3-pbkdf2
Accepted password length	The minimum and maximum password length

Label	Description
Credits for each character class	The maximum number of credits given for each character class
Number of required characters per class	The minimum number of characters for each character classes that is required in a password: uppercase, lowercase, numeric, or special character
Minimum number of required character classes	The number of different character classes that is required in a password: uppercase, lowercase, numeric, or special character
Required distance with previous password	The minimum number of characters required to be different in the new password from the old password.
Allow consecutively repeating a character	The number of times the same character is allowed to be repeated consecutively in a new command
Allow passwords containing username	Displays whether the username is allowed as part of the password
Palindrome allowed	Displays whether palindromes are allowed as part of the password

profile

Syntax

profile *user-profile-name*

Context

show>system>security

Description

This command displays user profile information.

If the *user-profile-name* is not specified, then information for all profiles is displayed.

Parameters

user-profile-name

displays information for the specified user profile

Output

The following output is an example of user profile information, and Table 21: User profile field descriptions describes the fields.

Output example

```
A:ALU-7# show system security profile administrative
===============================================================================
User Profile
===============================================================================
User Profile : administrative
Def. Action  : permit-all
LI           : no
-------------------------------------------------------------------------------
Entry        : 10
Description  :
Match Command: configure system security
Action       : permit
-------------------------------------------------------------------------------
Entry        : 20
Description  :
Match Command: show system security
Action       : permit
-------------------------------------------------------------------------------
No. of profiles: 1
===============================================================================
A:ALU-7#
```

Table 21: User profile field descriptions

Label	Description
User Profile	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	The entry ID in a policy or filter table
Description	Displays the text string describing the entry
Match Command	Displays the command or subtree commands in subordinate command levels
Action	Permit all: Commands matching the entry command match criteria are permitted
	Deny: Commands not matching the entry command match criteria are not permitted
No. of profiles	The total number of profiles listed

source-address

Syntax

source-address

Context

show>system>security

Description

This command displays the source address configured for applications.

Output

The following output is an example of source address information, and Table 22: Source address field descriptions describes the fields.

Output example

```
A:ALU-1# 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:ALU-1#
```

Table 22: Source address field descriptions

Label	Description
Application	The source-address application
IP address: Interface Name	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

Description

This command displays all the SSH sessions as well as the SSH status and fingerprint. The type of SSH application (CLI, SCP, or SFTP) is indicated for each SSH connection.

Output

The following output is an example of SSH information for an SSH server, and Table 23: SSH field descriptions describes the fields.

Output example

```
*A:7705:Dut-C# show system security ssh

===============================================================================
SSH Server
===============================================================================
Administrative State      : Enabled
Operational State         : Up
Preserve Key              : Disabled
Key-re-exchange           : 60 minutes / 1024 MB

SSH Protocol Version 2    : Enabled
DSA Host Key Fingerprint  : MD5:0a:89:df:09:d8:8c:c4:0d:6c:dc:42:28:79:f9:a1:cf
                            SHA256:VY42oECtkK3Qy+H+FMKShDzjqGKFlo/cxCdfemVNfwE
RSA Host Key Fingerprint  : MD5:8f:cf:0e:5e:48:1b:5d:ce:1a:fb:f6:15:57:1b:82:ac
                            SHA256:DEf9VOKmUz0rxRxhxoCmWs2E+Ny9ryVCADdornzCk/I
-------------------------------------------------------------------------------
Connection                                          ConnectionID
   Username                                         ConnectionStatus
   RouterInstance                                   Key-re-exchange
   Version   KEX
             Cipher
             MAC
   SessionID                 ChannelID   ServerName  ChannelStatus
-------------------------------------------------------------------------------
192.168.192.29                                      14
   admin                                            connected
   management                                       60 minutes / 1024 MB
   SSHv2     diffie-hellman-group-exchange-sha1
             aes128-ctr
             hmac-sha1
   16                        0           cli         connected
   17                        1           cli         connected
   18                        2           cli         connected
-------------------------------------------------------------------------------
192.168.192.29                                      17
   admin                                            connected
   management                                       60 minutes / 1024 MB
   SSHv2     diffie-hellman-group-exchange-sha1
             aes128-ctr
             hmac-sha1
   21                        0           sftp        connected
-------------------------------------------------------------------------------
Number of SSH connections : 2
Number of SSH sessions    : 4
===============================================================================
*A:7705
```

Table 23: SSH field descriptions

Label	Description
Administrative State	The administrative state of the SSH server: enabled or disabled
Operational State	The operational state of the SSH server: up or down
Preserve Key	The **preserve-key** configuration: enabled or disabled
Key-re-exchange	The maximum number of minutes elapsed or maximum number of megabytes transmitted before a key re-exchange is initiated
SSH Protocol Version 2	The SSHv2 configuration: enabled or disabled
DSA Host Key Fingerprint RSA Host Key Fingerprint	The key fingerprint is the digital signal algorithm (DSA) or Rivest, Shamir, and Adleman (RSA) host server's identity. Clients trying to connect to the server verify the server fingerprint. If the server fingerprint is not known, the client will get a warning message that the server may be spoofed and they will not be allowed to log in until the administrator fixes the issue. The MD5 and SHA 256 versions of the keys are supported.
Connection	The IP address of the connected routers (remote client)
ConnectionID	The SSH connection identifier
Username	The name of the user
ConnectionStatus	The status of the SSH connection: connected or disconnected
RouterInstance	The router instance used to establish the connection, either management or base
Key-re-exchange	The number of minutes or the number of megabytes transmitted after which a key re-exchange should occur for this connection
Version	SSHv2
KEX	The KEX algorithm used by the SSH session
Cipher	The cipher used by the SSH session
MAC	The MAC algorithm used by the SSH session
SessionID	The identifier for the session
ChannelID	The identifier for the channel

Label	Description
ServerName	The name of the server. For an SSH session, the value is cli. For an SFTP session, the value is sftp.
ChannelStatus	The status of the channel: connected or disconnected
Number of SSH connections	The total number of SSH connections
Number of SSH sessions	The total number of SSH sessions

cert-profile

Syntax

cert-profile *name* **association**

cert-profile [*name*]

cert-profile *name* **entry** *1..8*

Context

show>system>security>tls

Description

This command displays information about TLS certificate profiles.

Parameters

name

the name of a certificate profile for which to display information

association

displays TLS client profiles that are associated with the certificate profile

1..8

Values 1 to 8

Output

The following outputs are examples of client certificate profile information.

Output example

```
*A:7705# show system security tls cert-profile

===============================================================================
Certificate Profile
===============================================================================
Certificate Profile Name          AdminState  OperState  OperFlags
-------------------------------------------------------------------------------
certProfile1                      up          up
```

```
===============================================================================
```

```
A:7705# show system security tls cert-profile "certProfile1"

===============================================================================
Certificate Profile Entry "certProfile1"
===============================================================================
Id  Certificate File Name     Key File Name             Status Flags
-------------------------------------------------------------------------------
1   sarcert1                  sarkey1
===============================================================================
```

```
*A:7705# show system security tls cert-profile "certProfile1" entry 1

===============================================================================
TLS Certificate Profile: "certProfile1" Entry: 1 Detail
===============================================================================
Certificate File : sarcert1
Key File         : sarkey1
Status Flags     : (Not Specified)
===============================================================================
```

```
*A:7705# show system security tls cert-profile "certProfile1" association

===============================================================================
TLS Client Profiles using cert-profile "certProfile1"
===============================================================================
TLS Client Profile Name
-------------------------------------------------------------------------------
tlsClientProfile
-------------------------------------------------------------------------------
Number of TLS Client Profile entries: 1
===============================================================================
```

client-tls-profile

Syntax

client-tls-profile [*client-tls-profile*]

client-tls-profile *client-tls-profile* **association**

client-tls-profile *client-tls-profile* [**connections**]

Context

show>system>security>tls

Description

This command displays TLS client profile information.

Parameters

client-tls-profile

the name of the client TLS profile

association

displays TLS certificate profiles that are associated with the TLS client profile

connections

displays active TLS connections using the TLS client profile

Output

The following outputs are examples of TLS client profile information.

Output example

```
*A:7705# show system security tls client-tls-profile "tlsClientProfile"

===============================================================================
Client Profile Entry "tlsClientProfile"
===============================================================================
Cipher List Name             : tlsClientCipherList
Certificate Profile Name     : certProfile1
Trust Anchor Profile Name    : trustAnchorProfile1
===============================================================================
```

```
A:7705:Dut-A# show system security tls client-tls-profile "tlsClientProfile" connections

===============================================================================
Active TLS connections using client-tls-profile "tlsClientProfile"
===============================================================================
     Cipher                       Client Signature       Server Signature
       Matched Trust Anchor         Server IP
-------------------------------------------------------------------------------
Pcep
1    AES_128_CCM_8_SHA256         RSASSA-PSS-SHA256      RSASSA-PSS-SHA256
       rootCA                       10.20.1.4:4189
-------------------------------------------------------------------------------
Number of TLS connections: 1
===============================================================================
```

trust-anchor-profile

Syntax

trust-anchor-profile *trust-anchor-profile* **association**

trust-anchor-profile [*trust-anchor-profile*]

Context

show>system>security>tls

Description

This command displays information about TLS client profiles that are using the specified TLS trust anchor profile.

Parameters

trust-anchor-profile

specifies the trust anchor profile, up to 32 characters

association

displays TLS profiles that are associated with the trust anchor profile

Output

The following outputs are examples of trust anchor profile information.

Output example

```
*A:7705# show system security tls trust-anchor-profile
===============================================================================
Trust Anchor Profile Information
===============================================================================
Name                                            CA Profiles Down
-------------------------------------------------------------------------------
trustAnchorProfile1                             0
===============================================================================
```

```
*A:7705# show system security tls trust-anchor-profile "trustAnchorProfile1"
===============================================================================
CA-profile List for Trust Anchor "trustAnchorProfile1"
===============================================================================
CA Profile Name                                 AdminState     OperState
-------------------------------------------------------------------------------
rootCA                                          up             up
===============================================================================
```

```
*A:7705:Dut-A# show system security tls trust-anchor-profile "trustAnchorProfile1" association
===============================================================================
TLS Client Profiles using trust-anchor-profile trustAnchorProfile1
===============================================================================
TLS Client Profile Name
-------------------------------------------------------------------------------
tlsClientProfile
-------------------------------------------------------------------------------
Number of TLS Client Profile entries: 1
===============================================================================
```

user

Syntax

user [*user-id*] [**detail**]

user [*user-id*] **lockout**

Context

show>system>security

Description

This command displays user registration and security information. You can clear lockouts for users with the lockout command.

If no command line options are specified, summary information for all users displays.

Parameters

user-id

displays information for the specified user

Default all users

detail

displays detailed user information to the summary output

lockout

displays information about users that are currently locked out for too many failed login attempts

Output

The following output is an example of user information, and Table 24: User field descriptions describes the fields.

Note: Bluetooth (bt), gRPC (gc), LI (li), and NETCONF (nc) are not supported on the 7705 SAR and appear as "--" in the **show system security user detail** command output.

Output example

```
*A:7705:Dut-C>config>system>security# show system security user "test" detail

===============================================================================
Users
===============================================================================
User ID      New Access                          Password Login   Failed Local
             Pwd Permissions                     Expires  Attempt Logins Conf
-------------------------------------------------------------------------------
test         n   -- -- -- -- -- -- -- -- sc --    never    0       0      y
-------------------------------------------------------------------------------
Number of users : 1
Permissions: (bt) Bluetooth, (cc) Console port CLI, (fp) FTP, (gc) gRPC,
             (li) LI, (nc) NETCONF, (sp) SCP/SFTP, (sn) SNMP, (sc) SSH CLI,
             (tc) Telnet CLI
===============================================================================

===============================================================================
User Configuration Detail
===============================================================================
===============================================================================
user id            : test
-------------------------------------------------------------------------------
console parameters
-------------------------------------------------------------------------------
new pw required    : no                cannot change pw   : no
home directory     :
restricted to home : yes
save when restrict*: yes
login exec file    :
```

```
profile            : default
locked-out         : no
-------------------------------------------------------------------------------
snmp parameters
-------------------------------------------------------------------------------
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:7705:Dut-C>config>system>security#
```

```
ALU-7# show system security user lockout
===============================================================================
Currently Failed Login Attempts
===============================================================================
User ID        Remaining Login attempts      Remaining Lockout Time (min:sec)
-------------------------------------------------------------------------------
jason123               N/A                                 9:56
-------------------------------------------------------------------------------
Number of users : 1
===============================================================================
```

Table 24: User field descriptions

Label	Description
Users	
User ID	The name of a system user
New Pwd	Indicates whether the user must change their password at the next login: y or n
Access Permissions	bt Indicates whether the user is authorized for Bluetooth access (not supported on the 7705 SAR and always displays "--")
	cc Indicates whether the user is authorized for console port CLI access
	fp Indicates whether the user is authorized for FTP access
	gc Indicates whether the user is authorized for gRPC access (not supported on the 7705 SAR and always displays "--")
	li Indicates whether the user is authorized for lawful intercept (LI) access (not supported on the 7705 SAR and always displays "--")
	nc Indicates whether the user is authorized for NETCONF access (not supported on the 7705 SAR and always displays "--")

Label	Description
	sp Indicates whether the user is authorized for SCP/SFTP access
	sn Indicates whether the user is authorized for SNMP access
	sc Indicates whether the user is authorized for SSH CLI access
	tc Indicates whether the user is authorized for Telnet CLI access
Password Expires	The number of days the user has left before they must change their login password
Login Attempt	The number of times the user has attempted to log in regardless of whether the login succeeded or failed
Failed Logins	The number of unsuccessful login attempts
Local Conf	Indicates whether password authentication is based on the local password database: y or n
Number of users	The total number of listed users
User Configuration Detail	
console parameters	
new pw required	Indicates whether the user must change their password at the next login: yes or no
cannot change pw	Indicates whether the user is prevented from changing their password: yes or no
home directory	The local home directory for the user for both console and FTP access
restricted to home	Indicates whether the user is restricted from navigating to a directory higher in the directory tree on the home directory device: yes or no
save when restricted	Indicates whether configuration save operations are allowed when the user is restricted to home: yes or no
login exec file	The user’s login exec file, which executes whenever the user successfully logs in to a console session
profile	The security profiles associated with the user

Label	Description
locked-out	Indicates whether the user is locked out, and if they are locked out, how much time remains before the user can attempt to log in to the node again
snmp parameters	
auth protocol	The SNMPv3 authentication protocol
auth key	The SNMPv3 authentication key
privacy protocol	The SNMPv3 privacy protocol
privacy key	The SNMPv3 privacy key
group	The group to which the protocols apply
Currently Failed Login Attempts	
Remaining Login attempts	The number of login attempts remaining before the user is locked out
Remaining Lockout Time (min:sec)	The time remaining before the lockout time expires and the user can attempt another login

With the support of PKI on the 7705 SAR as an SSH server, the authentication process can be done via PKI or password. SSH clients usually authenticate via PKI and password if PKI is configured on the client. In this case, PKI takes precedence over password authentication in most clients.

All client authentications are logged and displayed in the **show>system>security>user detail** output. The following table shows the rules where pass and fail attempts are logged.

Table 25: Pass/fail login attempts

Authentication order	Client (for example, PuTTY)	Server (for example, 7705 SAR)		CLI show system security attempts	
	Private key programmed	Public key configured	Password configured	Login attempts	Failed logins
1. Public key 2. Password	Yes	Yes	N/A	Increment	—
	Yes	Yes (if no match between client and server, go to password)	Yes	Increment	—
	Yes	No	Yes	Increment	—
	No	N/A	Yes	Increment	—
	No	N/A	No	—	Increment

Authentication order	Client (for example, PuTTY)	Server (for example, 7705 SAR)		CLI show system security attempts	
	Private key programmed	Public key configured	Password configured	Login attempts	Failed logins
1. Public key (only)	Yes	Yes	N/A	Increment	—
	Yes	Yes (if no match between client and server, go to password)	N/A	—	Increment
	Yes	No	N/A	—	Increment
	No	N/A	N/A	—	Increment

view

Syntax

view [*view-name*] [**detail**] [**capabilities**]

Context

show>system>security

Description

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

Parameters

view-name

specifies the name of the view to display. If no view name is specified, the complete list of views displays.

detail

displays detailed view information

Output

The following output is an example of view information, and Table 26: View field descriptions describes the fields.

Output example

```
A:ALU-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       1.3.6.1.2.1.31                                  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
vprn-view       1.3.6.1.2.1.2                                   included
vprn-view       1.3.6.1.2.1.4                                   included
vprn-view       1.3.6.1.2.1.5                                   included
vprn-view       1.3.6.1.2.1.6                                   included
vprn-view       1.3.6.1.2.1.7                                   included
vprn-view       1.3.6.1.2.1.23                                  included
vprn-view       1.3.6.1.2.1.31                                  included
vprn-view       1.3.6.1.2.1.77                                  included
vprn-view       1.3.6.1.4.1.6527.3.1.2.3.7                      included
vprn-view       1.3.6.1.4.1.6527.3.1.2.3.11                     included
vprn-view       1.3.6.1.4.1.6527.3.1.2.20.1                     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
on-security     2                               00000000        included
-------------------------------------------------------------------------------
No. of Views: 30
===============================================================================
A:ALU-48#
```

Table 26: View field descriptions

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

3.11.2.3.2 Login control show commands

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

users

Syntax

users

Context

show

Description

This command displays console user login and connection information.

Output

The following output is an example of user login information, and Table 27: Users field descriptions describes the fields.

Output example

```
*A:7705:Dut-C# show users
===============================================================================
Username                                        Type
    From
    Router instance
    Connection ID                               Login time
        Session ID            SSH Channel ID        Idle time
===============================================================================
                                                Console
    --
    --
    6                                             --
        6                     --                  0d 07:11:00  --
-------------------------------------------------------------------------------
admin                                           Telnet
    192.168.192.29
    management
    16                                          28SEP2023 21:03:11
       #20                    --                  0d 00:00:00  --
-------------------------------------------------------------------------------
admin                                           Telnet
    192.168.192.30
    management
    12                                          28SEP2023 16:58:33
        14                    --                  0d 04:40:43  --
-------------------------------------------------------------------------------
admin                                           SSHv2
    192.168.192.29
    management
    14                                          28SEP2023 20:29:54
        16                    0                   0d 00:00:25  --
        17                    1                   0d 00:17:59  --
        18                    2                   0d 01:17:08  --
-------------------------------------------------------------------------------
admin                                           SSHv2
    192.168.192.29
    management
    17                                            --
        21                    0                   0d 00:11:18  --
```

```
-------------------------------------------------------------------------------
admin                                               FTP
    192.168.192.29
    management
    18                                              28SEP2023 21:46:59
        22                      --                      0d 00:00:04  --
-------------------------------------------------------------------------------
Number of users: 5
Number of sessions: 7
'#' indicates the current active session
===============================================================================
*A:7705:Dut-C#
```

Table 27: Users field descriptions

Label	Description
Username	The name of the user
Type	The type of connection: console, Telnet, FTP, SFTP, SSH, or MCT The console session is always displayed but does not count against the number of sessions unless a user is logged in at the console. If no one is logged in at the console, the Username field is blank.
From	The originating IP address
Router instance	The routing instance used to establish the connection, either management or base
Connection ID	The identifier for the connection
Login time	The time the user logged in
Session ID	The identifier for the session
SSH Channel ID	The SSH channel identifier
Idle time	The amount of idle time for a specific login
Number of users	The total number of users logged in
Number of sessions	The total number of sessions across all FTP, SFTP, SSH, Telnet, and MCT connections

3.11.2.4 Clear commands

lockout

Syntax

lockout all

lockout user *user-name*

Context

admin>clear

Description

This command clears a security lockout for a specific user, or for all users, after they have been locked out for failing too many login attempts.

Parameters

all

clears lockouts for all users

name

specifies a username

password-history

Syntax

password-history all

password-history user *user-name*

Context

admin>clear

Description

This command clears old passwords for a specific user or for all users.

Parameters

all

clears password history for all users

name

specifies a username

statistics

Syntax

statistics [**interface** *ip-int-name* | *ip-address*]

Context

clear>router>authentication

Description

This command clears authentication statistics.

Parameters

ip-int-name

clears the authentication statistics for the specified interface name. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

ip-address

clears the authentication statistics for the specified IP address

3.11.2.5 Monitor commands

cpm-filter

Syntax

cpm-filter

Context

monitor

Description

This command displays monitor command output for CPM filters.

management-access-filter

Syntax

management-access-filter

Context

monitor

Description

This command enables the context to monitor management access filters.

ip

Syntax

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

Context

monitor>cpm-filter

monitor>management-access-filter

Description

This command enables IP filter monitoring. The statistical information for the specified IP filter entry is displayed at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the specified IP filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous screen output.

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

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

Parameters

entry-id

displays information for the specified filter entry ID

Values 1 to 120 (CPM filter)

1 to 9999 (management access filter)

seconds

configures the interval for each display in seconds

Values 3 to 60

Default 10

repeat

configures how many times the command is repeated

Values 1 to 999

Default 10

absolute

displays raw statistics, without processing. No calculations are performed on the delta or rate statistics.

rate

displays the rate per second for each statistic instead of the delta

ipv6

Syntax

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

Context

monitor>cpm-filter

monitor>management-access-filter

Description

This command enables IPv6 filter monitoring. The statistical information for the specified IPv6 filter entry is displayed at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the specified IPv6 filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous screen output.

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

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

Parameters

entry-id

displays information for the specified filter entry ID

Values 1 to 120 (CPM filter)

1 to 9999 (management access filter)

seconds

configures the interval for each display in seconds

Values 3 to 60

Default 10

repeat

configures how many times the command is repeated

Values 1 to 999

Default 10

absolute

displays raw statistics, without processing. No calculations are performed on the delta or rate statistics.

rate

displays the rate per second for each statistic instead of the delta

mac

Syntax

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

Context

monitor>cpm-filter

monitor>management-access-filter

Description

This command enables MAC filter monitoring. The statistical information for the specified MAC filter entry is displayed at the configured interval until the configured count is reached.

The first screen displays the current statistics related to the specified MAC filter. The subsequent statistical information listed for each interval is displayed as a delta to the previous screen output.

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

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

Parameters

entry-id

displays information for the specified filter entry ID

Values 1 to 120 (CPM filter)

1 to 9999 (management access filter)

seconds

configures the interval for each display in seconds

Values 3 to 60

Default 10

repeat

configures how many times the command is repeated

Values 1 to 999

Default 10

absolute

displays raw statistics, without processing. No calculations are performed on the delta or rate statistics.

rate

displays the rate per second for each statistic instead of the delta

3.11.2.6 Debug commands

radius

Syntax

radius [**detail**] [**hex**]

no radius

Context

debug

Description

This command enables debugging for RADIUS connections.

The **no** form of the command disables the debugging.

Parameters

detail

displays detailed output

hex

displays the packet dump in hexadecimal format

4 SNMP

This chapter provides information to configure SNMP.

Topics in this chapter include:

- SNMP overview
- SNMP versions
- Configuration notes
- Configuring SNMP with CLI
- SNMP command reference

4.1 SNMP overview

4.1.1 SNMP architecture

The Service Assurance Manager (SAM) consists of two elements: managers and agents. The manager is the entity through which network management tasks are facilitated. An agent is a software module integrated into the operating system of the managed device that communicates with the network manager. 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 that 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 managed device (for example, the 7705 SAR router).

SNMP is supported on network hosts using the IPv4 and IPv6 protocols.

4.1.2 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's management information consists of a set of network objects that can be managed with SNMP. Object identifiers are unique object names that are organized in a hierarchical tree structure. The main branches are defined by the Internet Engineering Task Force (IETF). When requested, the Internet Assigned Numbers Authority (IANA) assigns a unique branch for use by a private organization or company. The branch assigned to the 7705 SAR 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 the 7705 SAR.

4.1.3 SNMP versions

The agent supports multiple versions of the SNMP protocol:

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.

  SNMPv1 provides access control for communities and uses a community string match for authentication.
- SNMPv2c uses a community string match for authentication.
- SNMP Version 3 (SNMPv3) provides access control for users. In SNMPv3, User-based Security Model (USM) defines the user authentication and encryption features. The 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.

4.1.4 Management information access control

By default, the 7705 SAR 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 are standard read-only, read-write, and read-write-all access groups and views that can simply be assigned community strings. In order to implement SNMP with security features, security models, security levels, and USM communities must be explicitly configured. Optionally, additional views that specify more specific OIDs (MIB objects in the subtree) can be configured.

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

The use of community strings 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 allow access to the agent on the 7705 SAR router.

The 7705 SAR 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

4.1.5 User-based security model community strings

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.

4.1.6 Views

Views control the access to a managed object. The total MIB of a 7705 SAR 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 allowed, such as read, write, or notify.

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

Predefined views are available that are particularly useful when configuring SNMPv1 and SNMPv2c.

The SNMP agent associates SNMPv1 and SNMPv2c community strings with an SNMPv3 view.

4.1.7 Access groups

Access groups associate a user group and a security model with 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 is a template that defines a combination of access privileges and views. A group can be associated with 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 the security requirements.

4.1.8 Users

By default, authentication and encryption parameters are not configured. Authentication parameters that a user must use in order to be validated by the 7705 SAR can be modified. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with.

User access and authentication privileges must be explicitly configured. In a user configuration, a user is associated with an access group, which is a collection of users who have common access privileges and views.

4.2 SNMP versions

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

To implement SNMPv3, an authentication and encryption method must be assigned to a user in order to be validated by the 7705 SAR. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

4.2.1 SNMPv3 authentication and privacy protocols

The following SNMPv3 authentication protocols are supported:

- HMAC -MD5-96
- HMAC-SHA-96
- HMAC-SHA-224
- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512

The following SNMPv3 privacy protocols are supported:

- CBC-DES
- CFB128-AES-128
- CFB128-AES-192
- CFB128-AES-256

4.3 Configuration notes

The following are SNMP configuration guidelines and restrictions:

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

  In order to enable SNMP, the portions of the configuration that failed to load must be initialized properly. Start SNMP with the **config>system>snmp>no shutdown** 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 the configuration is not saved and the system is not rebooted, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

4.4 Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

- SNMP configuration overview
- Basic SNMP security configuration
- Configuring SNMP components

4.5 SNMP configuration overview

This section describes how to configure SNMP components that apply to SNMPv1, SNMPv2c, and SNMPv3 on the 7705 SAR:

- Configuring SNMPv1 and SNMPv2c
- Configuring SNMPv3

4.5.1 Configuring SNMPv1 and SNMPv2c

The 7705 SAR router is based on SNMPv3. To use 7705 SAR routers with SNMPv1 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.

4.5.2 Configuring SNMPv3

The 7705 SAR implements SNMPv3. If security features other than the default views are required, the following parameters must be configured:

- views
- access groups
- SNMP users

4.6 Basic SNMP security configuration

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

For SNMPv1 and SNMPv2c, configure community string parameters.

For SNMPv3:

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

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

```
ALU-1>config>system>security>snmp# info detail
----------------------------------------------
                view iso subtree 1
                    mask ff type included
                exit
                view "mgmt-view" subtree 1.3.6.1.2.1.2
                    mask ff type excluded
                exit
                view "mgmt-view" subtree 1.3.6.1.2.1.4
                    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-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
```

4.7 Configuring SNMP components

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

- Configuring a community string
- Configuring view options

- Configuring access options
- Configuring USM community options
- Configuring other SNMP parameters

CLI syntax:

```
config>system>security>snmp
    access group group-name security-model security-model security-
level security-level [context context-name [prefix-match]] [read view-
name-1] [write view-name-2] [notify view-name-3]
    attempts [count] [time minutes1] [lockout minutes2]
    community community-string [hash | hash2] access-permissions
 [version SNMP-version]
    usm-community community-string [hash | hash2] group group-name
    view view-name [subtree oid-value]
        mask mask-value [type {included | excluded}]
```

4.7.1 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 allow access to the agent. The access granted with a community string is restricted to the scope of the configured group.

One or more of the following 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
- assignment of a unique community string to the management router or management VPLS
- the SNMP version: SNMPv1, SNMPv2c, or both

Default access features are preconfigured by the agent for SNMPv1 and SNMPv2c.

Use the following CLI syntax to configure community options:

CLI syntax:

```
config>system>security>snmp
    community community-string [hash | hash2] access-permissions
 [version SNMP-version]
```

The following example displays community string command usage:

Example:

```
config>system>security# snmp
config>system>security>snmp# community private hash2 rwa version both
config>system>security>snmp# community public hash2 r version v2c
```

The following example displays the SNMP community configuration:

```
ALU-1>config>system>security>snmp# info
----------------------------------------------------
     community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
     community "Lla.RtAyRW2" hash2 r version v2c
----------------------------------------------------
ALU-1>config>system>security>snmp#
```

4.7.2 Configuring view options

Use the following CLI syntax to configure view options:

CLI syntax:

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

The following example displays view command usage:

Example:

```
config>system>security>snmp# view testview subtree 1
config>system>security>snmp>view$ mask ff type included
config>system>security>snmp>view$ exit
config>system>security>snmp# view testview subtree 1.3.6.1.2
config>system>security>snmp>view$ mask ff type X
config>system>security>snmp>view$ exit
```

The following example displays the view configuration:

```
ALU-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
                community "private" rwa version both
                community "public" r version v2c
----------------------------------------------
ALU-1>config>system>security>snmp#
```

4.7.3 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 SNMPv2c. An access group is defined by a unique combination of the group name, security model, and security level.

Use the following CLI syntax to configure access features:

CLI syntax:

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

The following example displays access command usage:

Example:

```
ALU-1>config>system>security>snmp# access group
testgroup security-model usm security-level auth-no-privacy read
 testview write testview notify testview
```

The following example displays the access configuration with the view configurations.

```
ALU-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 “testgroup” security-model usm security-level auth-no
-privacy read “testview” write “testview” notify “testview”
                community "public" r version both
----------------------------------------------
```

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

CLI syntax:

```
config>system>security# user user-name
    access [ftp] [snmp] [console]
    snmp
        authentication none
        authentication authentication-protocol authentication-key
 [privacy none] [hash | hash2]
        authentication authentication-protocol authentication-key
 privacy privacy-protocol privacy-key [hash|hash2]
        no authentication
    group group-name
```

The following example displays user security command usage:

Example:

```
config>system>security# user testuser
config>system>security>user$ access snmp
config>system>security>user# snmp
config>system>security>user>snmp# authentication hash hmac-md5-96
 e14672e71d3e96e7a1e19472527ee969 privacy none
config>system>security>user>snmp# group testgroup
config>system>security>user>snmp# exit
config>system>security>user# exit
```

The following example displays the user’s SNMP configuration.

```
ALU-1>config>system>security# info
----------------------------------------------
    user "testuser"
        access snmp
        snmp
            authentication hash hmac-md5-96  e14672e71d3e96e7a1e19472527ee969
privacy none
            group testgroup
        exit
    exit
...
----------------------------------------------
ALU-1>config>system>security#
```

4.7.4 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 7705 SAR implementation of SNMP uses SNMPv3. To implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

CLI syntax:

```
config>system>security>snmp
    usm-community community-string [hash | hash2] group group-name
```

The following example displays USM community string command usage. The group "testgroup" was configured in the **config>system>security>snmp>access** CLI context.

Example:

```
config>system>security>snmp# usm-community "test" hash2 group
 "testgroup"
```

The following example displays the SNMP community configuration:

```
ALU-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 testgroup security-model usm security-level auth-no
-privacy read testview write testview notify testview
                community "private" hash2 rwa version both
                community "public" hash r version v2c
                usm-community "test" group "testgroup"
----------------------------------------------
ALU-1>config>system>security>snmp#
```

4.7.5 Configuring other SNMP parameters

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

CLI syntax:

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

The following example displays the system SNMP default values:

```
ALU-104>config>system>snmp# info detail
----------------------------------------------
```

```
            shutdown
            engineID "0000xxxx000000000xxxxx00"
            packet-size 1500
            general-port 161
-----------------------------------------------
ALU-104>config>system>snmp#
```

4.8 SNMP command reference

4.8.1 Command hierarchies

- Configuration commands
  - SNMP system commands
  - SNMP security commands
- Show commands

4.8.1.1 Configuration commands

4.8.1.1.1 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
            - streaming
                -   [no] shutdown
```

4.8.1.1.2 SNMP security commands

```
config
- system
        - security
            - snmp
                - access group group-name security-model security-model security-level
 security-level [context context-name [prefix-match]] [read view-name-1] [write view-name-2]
 [notify view-name-3]
                - 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]
                - 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 command reference section for CLI syntax and command descriptions.

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

4.8.1.2 Show commands

```
show
- snmp
        - counters
        - streaming
            - counters
- system
        - information
        - security
            - access-group [group-name]
            - communities
            - user [user-id] [detail]
            - view [view-name] [capabilities] [detail]
```

4.8.2 Command descriptions

- Configuration commands
- Show commands

4.8.2.1 Configuration commands

- SNMP system commands
- SNMP security commands

4.8.2.1.1 SNMP system commands

snmp

Syntax

snmp

Context

config>system

Description

This command enables the context to configure SNMP parameters.

engineID

Syntax

[**no**] **engineID** *engine-id*

Context

config>system>snmp

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 in the **config**>**system**>**snmp**>**engineID** *engine-id* context, the current configuration must be saved and a reboot must be executed. If the configuration is not saved and the system is not rebooted, the previously configured SNMP communities and logger trap-destination notify communities will not be valid for the new engine ID.

Caution: In conformance with IETF standard RFC 3414, *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 engine ID. Changing the SNMP engine ID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable. If the SNMP engine ID is changed, the SNMP hash keys must be reconfigured.

This command could be used, for example, 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 engine ID.

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

Default

the engine ID is system-generated

Parameters

engine-id

an identifier from 10 to 64 hexadecimal digits (5 to 32 octet number), uniquely identifying this SNMPv3 node. This string is used to access this node from a remote host with SNMPv3.

general-port

Syntax

general-port *port-number*

no general-port

Context

config>system>snmp

Description

This command configures the port number used by this node to receive SNMP request messages and to send replies. SNMP notifications generated by the agent are sent from the port specified in the **config**>**log**>**snmp-trap-group**>**trap-target** command.

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

Default

161

Parameters

port-number

the port number used to send SNMP traffic other than traps

Values 1 to 65535 (decimal)

packet-size

Syntax

packet-size *bytes*

no packet-size

Context

config>system>snmp

Description

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

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

Default

1500 bytes

Parameters

bytes

the SNMP packet size in bytes

Values 484 to 9216

shutdown

Syntax

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

Context

config>system>snmp

Description

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

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

The **no** form of the command administratively enables SNMP.

Default

no shutdown

streaming

Syntax

streaming

Context

config>system>snmp

Description

This command enables the proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes. In higher-latency networks, synchronizing router MIBs from network management via streaming takes less time than synchronizing via classic SNMP UDP requests. Streaming operates on TCP port 1491 and runs over IPv4 or IPv6.

shutdown

Syntax

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

Context

config>system>snmp>streaming

Description

This command administratively disables the proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes.

The **no** form of the command administratively re-enables SNMP request/response bundling and the TCP-based transport mechanism.

Default

shutdown

4.8.2.1.2 SNMP security commands

snmp

Syntax

snmp

Context

config>system>security

Description

This command enables the context to configure SNMPv1, SNMPv2c, and SNMPv3 parameters

access group

Syntax

[**no**] **access group** *group-name* **security-model** {**snmpv1** | **snmpv2c** | **usm**} **security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}[**context** *context-name* [**prefix-match** {**exact** | **prefix**}]][**read** *view-name-1*][**write** *view-name-2*][**notify** *view-name-3*]

Context

config>system>security>snmp

Description

This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2c. 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 community).

Default access group configurations cannot be modified or deleted.

To remove the user group with associated security models and security levels, use the command **no access group** *group-name*.

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

Default

n/a

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 and no privacy (encryption) is required. When configuring the user's authentication, select the **none** option.

security-level auth-no-privacy

specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the group and the user must be configured for authentication.

security-level privacy

specifies that both authentication and privacy (encryption) is required. When this option is configured, both the group and the user must be configured for authentication. The user must also be configured for privacy.

context-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).

prefix-match

specifies the context-name prefix-match keywords, exact or prefix

Default exact

read *view-name-1*

specifies the keyword and variable of the view to read the MIB objects. This command must be configured for each view to which the group has read access.

Values up to 32 characters

write *view-name-2*

specifies the keyword and variable of the view to configure the contents of the agent. This command must be configured for each view to which the group has write access.

Values up to 32 characters

notify *view-name-3*

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

Values up to 32 characters

attempts

Syntax

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

no attempts

Context

config>system>security>snmp

Description

This command configures a threshold value for the number of unsuccessful SNMP connection attempts allowed in a specified time frame. The command parameters are used to counter denial of service (DOS) attacks through SNMP.

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

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

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

Default

attempts 20 time 5 lockout 10

Parameters

count

the number of unsuccessful SNMP attempts allowed for the specified time

Values 1 to 64

Default 20

time *minutes1*

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

Values 0 to 60

Default 5

lockout *minutes2*

the lockout period, in minutes, during which the host is not allowed to log in. When the host exceeds the attempted count times in the specified time, then that host is locked out from any further login attempts for the configured time period.

Values 0 to 1440

Default 10

community

Syntax

community *community-string*[**hash** | **hash2**]*access-permissions*[**version** *SNMP-version*]

no community *community-string*[**hash** | **hash2**]

Context

config>system>security>snmp

Description

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

When configured, community implies a security model for SNMPv1 and SNMPv2c only.

For SNMPv3 security, the snmp command must be configured.

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

Default

n/a

Parameters

community-string

configures the SNMPv1/SNMPv2c community string

hash1 | hash2

configures the hashing scheme for the community string

access-permissions

defines the access permissions

Values

- 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 objects
- rwa – grants read and write access to all objects in the MIB, including security objects
- mgmt – assigns a unique SNMP community string to the management router
- vpls-mgmt – assigns a unique SNMP community string to the management virtual router

version

specifies the SNMP version

Values v1 | v2c | both

usm-community

Syntax

usm-community *community-string*[**hash** | **hash2**] **group** *group-name*

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

Context

config>system>security>snmp

Description

This command is used to associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

The 7705 SAR implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views that specify more specific OIDs (MIB objects in the subtree) can be configured.

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

Default

n/a

Parameters

community-string

configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used

hash1 | hash2

configures the hashing scheme for the community string

group

specifies the group that governs the access rights of this community string. This group must be configured first in the **config**>**system**>**security**>**snmp**>**access group** context.

group-name

specifies the group name

view

Syntax

view *view-name* **subtree** *oid-value*

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

Context

config>system>security>snmp

Description

This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.

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. The views configured with this command can subsequently be used in read, write, and notify commands that 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* command removes a sub-tree from the view name.

Default

no views are defined

Parameters

view-name

the 1 to 32 character view name

Default n/a

oid-value

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

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

mask

Syntax

mask *mask-value*[**type** {**included** | **excluded**}]

no mask

Context

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

Description

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

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

For example, the MIB subtree that represents MIB-II is 1.3.6.1.2.1. The mask that catches all MIB-II is 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 ones, are defined in this table. To determine if a particular object instance is in a particular MIB view, compare the object instance's object identifier (OID) with each of the MIB view's active entries in this table. If none match, then the

object instance is not in the MIB view. If one or more match, then the object instance is included in, or excluded from, the MIB view according to the value of vacmViewTreeFamilyType in the entry whose value of vacmViewTreeFamilySubtree has the most sub-identifiers.

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

Default

no mask

Parameters

mask-value

the mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view

The mask can be entered in either:

- hexadecimal format (for example, 0xfc)
- binary format (for example, 0b11111100)

Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.

Default all 1s

type {included | excluded}

specifies whether to include or exclude MIB subtree objects

included - all MIB subtree objects that are identified with a 1 in the mask are available in the view

excluded - all MIB subtree objects that are identified with a 1 in the mask are denied access in the view

Default included

4.8.2.2 Show commands

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

counters

Syntax

counters

Context

show>snmp

Description

This command displays SNMP counter 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 counters information, and Table 28: SNMP counters field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-1#
```

Table 28: SNMP counters field descriptions

Label	Description
in packets	The total number of messages delivered to SNMP from the transport service
in gets	The number of SNMP get request PDUs accepted and processed by SNMP
in getnexts	The number of SNMP get next PDUs accepted and processed by SNMP
in sets	The number of SNMP set request PDUs accepted and processed by SNMP
out packets	The total number of SNMP messages passed from SNMP to the transport service
out get responses	The number of SNMP get response PDUs generated by SNMP
out traps	The number of SNMP Trap PDUs generated by SNMP
variables requested	The number of MIB objects requested by SNMP

Label	Description
variables set	The number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs

streaming

Syntax

streaming

Context

show>snmp

Description

This command enables the context to display streaming counters information.

counters

Syntax

counters

Context

show>snmp>streaming

Description

This command displays counters information for the proprietary SNMP streaming protocol.

Output

The following output is an example of SNMP streaming counters information, and Table 29: SNMP streaming counters field descriptions describes the fields.

Output example

```
*A:custDoc sar8# show snmp streaming counters
===============================================================================
STREAMING counters:
===============================================================================
 in getTables   : 722
 in getManys    : 26
-------------------------------------------------------------------------------
 out responses  : 848
===============================================================================
```

Table 29: SNMP streaming counters field descriptions

Label	Description
in getTables	Displays the number of GetTable request packets received
in getManys	Displays the number of GetMany request packets received
out responses	Displays the number of response packets sent

information

Syntax

information

Context

show>system

Description

This command lists the SNMP configuration and statistics.

Output

The following output is an example of system information, and Table 30: System information field descriptions describes the fields.

Output example

```
A:7705:Dut-A# show system information
===============================================================================
System Information
===============================================================================
System Name            : A:7705:Dut-A
System Type            : 7705 SAR-8 v2
Chassis Topology       : Standalone
System Version         : B-0.0.I323
Crypto Module Version  :
 CPM: SARCM 3.0  DP: SARDCM 1.0
System Contact         : Fred Information Technology
System Location        : Bldg.1-floor 2-Room 201
System Coordinates     : N 85 58 23, W 34 56 12
System Active Slot     : A
System Up Time         : 1 days, 02:03:17.62 (hr:min:sec)

SNMP Port              : 161
SNMP Engine ID         : 0000197f00006883ff000000
SNMP Engine Boots      : 58
SNMP Max Message Size  : 1500
SNMP Admin State       : Enabled
SNMP Oper State        : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State        : OK

Tel/Tel6/SSH/FTP Admin : Enabled/Disabled/Enabled/Disabled
```

```
Tel/Tel6/SSH/FTP Oper  : Up/Down/Up/Down

BOF Source             : cf3:
Image Source           : primary
Config Source          : primary
Last Booted Config File: cf3:/config.cfg
Last Boot Cfg Version  : FRI APR 20 16:24:27 2007 UTC
Last Boot Config Header: # TiMOS-B-5.0.R3 both/hops NOKIA 7705 SAR #
                         Copyright (c) 2016 Nokia. All rights
                         reserved. # All use subject to applicable license
                         agreements. # Built on Wed Feb 13 19:45:00 EST 2016 by
                         builder in /rel5.0/R3/panos/main # Generated TUE
                         MAR 11 16:24:27 2016 UTC
Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-5.0.R3 both/hops NOKIA 7705 SAR #
                         Copyright (c) 2016 Nokia. All rights
                         reserved. # All use subject to applicable license
                         agreements. # Built on Wed Feb 13 19:45:00 EST 2016 by
                         builder in /rel5.0/R3/panos/main # Generated TUE
                         MAR 11 16:24:27 2016 UTC
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: Yes
User Last Modified     : admin
Time Last Modified     : 2016/03/19 10:03:09
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

Microwave S/W Package  : invalid

Management IP Addr     : 192.168.xxx.xxx/24
Primary DNS Server     : 192.168.xxx.xxx
Secondary DNS Server   : N/A
Tertiary DNS Server    : N/A
DNS Domain             : domain.com
DNS Resolve Preference : ipv4-only
BOF Static Routes      :
  To                   Next Hop
  192.xxx.0.0/16       192.xxx.1.1
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

ICMP Vendor Enhancement: Disabled
Eth QinQ Untagged SAP  : False
===============================================================================
A:7705:Dut-A#
```

Table 30: System information field descriptions

Label	Description
System Name	The configured system name
System Type	The 7705 SAR chassis model
Chassis Topology	The chassis setup – always Standalone

Label	Description
System Version	The version of the installed software load
Crypto Module Version	The cryptographic module in the release
System Contact	A text string that describes the system contact information
System Location	A text string that describes the system location
System Coordinates	A text string that describes the system coordinates
System Active Slot	The active CSM slot
System Up Time	The time since the last boot
SNMP Port	The port number used by this node to receive SNMP request messages and to send replies
SNMP Engine ID	The SNMP engine ID to uniquely identify the SNMPv3 node
SNMP Engine Boots	The number of times that the SNMP engine has booted
SNMP Max Message Size:	The maximum SNMP packet size generated by this node
SNMP Admin State	Enabled – SNMP is administratively enabled and running
	Disabled – SNMP is administratively shut down and not running
SNMP Oper State	Enabled – SNMP is operationally enabled
	Disabled – SNMP is operationally disabled
SNMP Index Boot Status	Persistent – system indexes are saved between reboots
	Not Persistent – system indexes are not saved between reboots
Tel/Tel6/SSH/FTP Admin	The administrative state of the Telnet, Telnet IPv6, SSH, and FTP sessions
Tel/Tel6/SSH/FTP Oper	The operational state of the Telnet, Telnet IPv6, SSH, and FTP sessions
BOF Source	The location of the BOF
Image Source	Primary – indicates that the directory location for runtime image file was loaded from the primary source
	Secondary – indicates that the directory location for runtime image file was loaded from the secondary source
	Tertiary – indicates that the directory location for runtime image file was loaded from the tertiary source

Label	Description
Config Source	Primary – indicates that the directory location for configuration file was loaded from the primary source
	Secondary – indicates that the directory location for configuration file was loaded from the secondary source
	Tertiary – indicates that the directory location for configuration file was loaded from the tertiary source
Last Booted Config File	The URL and filename of the last loaded configuration file
Last Boot Cfg Version	The date and time of the last boot
Last Boot Config Header	The header information such as image version, date built, date generated
Last Boot Index Version	The version of the persistence index file read when this CSM card was last rebooted
Last Boot Index Header	The header of the persistence index file read when this CSM card was last rebooted
Last Saved Config	The location and filename of the last saved configuration file
Time Last Saved	The date and time of the last time configuration file was saved
Changes Since Last Save	Yes – there are unsaved configuration file changes
	No – there are no unsaved configuration file changes
User Last Modified	The username of the user who last modified the configuration file
Time Last Modified	The date and time of the last modification
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL – the location and name of the CLI script file executed following successful completion of the boot-up configuration file execution
	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

Label	Description
	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
Microwave S/W Package	N/A
Management IP Addr	The management IP address and mask
Primary DNS Server	The IP address of the primary DNS server
Secondary DNS Server	The IP address of the secondary DNS server
Tertiary DNS Server	The IP address of the tertiary DNS server
DNS Domain	The DNS domain name of the node
DNS Resolve Preference	N/A
BOF Static Routes	To – the static route destination
	Next Hop – the next-hop IP address used to reach the destination
	Metric – displays the priority of this static route versus other static routes
	None – no static routes are configured
ATM Location ID	For ATM OAM loopbacks – the address of the network device referenced in the loopback request
ATM OAM Retry Up	N/A
ATM OAM Retry Down	N/A
ATM OAM Loopback Period	N/A
ICMP Vendor Enhancement	Enabled – inserts one-way timestamp in outbound SAA ICMP ping packets
	Disabled – one-way timestamping is not performed on outbound SAA ICMP ping packets
Eth QinQ untagged SAP	True: QinQ untagged SAPs are enabled
	False: QinQ untagged SAPs are disabled

access-group

Syntax

access-group [*group-name*]

Context

show>system>security

Description

This command displays access group information.

Parameters

group-name

the access group name

Output

The following output is an example of access group information, and Table 31: System access group field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-1#
```

```
A:ALU-1# show system security access-group snmp-ro
===============================================================================
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: 1
...
===============================================================================
```

```
A:ALU-1#
```

Table 31: System access group field descriptions

Label	Description
Group name	The access group name
Security model	The security model required to access the views configured in this node
Security level	The required authentication and privacy levels to access the views configured in this node
Read view	The view to read the MIB objects
Write view	The view to configure the contents of the agent
Notify view	The view to send a trap about MIB objects
No. of access groups	The total number of configured access groups

communities

Syntax

communities

Context

show>system>security

Description

This command lists SNMP communities and characteristics.

Output

The following output is an example of communities information, and Table 32: Communities field descriptions describes the fields.

Output example

```
A:ALU-1# show system security communities
===============================================================================
Communities
===============================================================================
community           access  view                version   group name
-------------------------------------------------------------------------------
private             rw      iso                 v1 v2c    snmp-rwa
cli-readonly        r       iso                 v2c       cli-readonly
cli-readwrite       rw      iso                 v2c       cli-readwrite
-------------------------------------------------------------------------------
No. of Communities: 3
===============================================================================
```

```
A:ALU-1#
```

Table 32: Communities field descriptions

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

user

Syntax

user [*user-id*][**detail**]

Context

show>system>security

Description

This command displays user information.

Parameters

user-id

the name of the user

detail

displays all information associated with the specified use

Output

The following output is an example of user information, and Table 33: User field descriptions describes the fields.

Output example

```
A:ALU-1# show system security user
===============================================================================
Users
===============================================================================
user id          New    User Permissions  Password    Login     Failed  Local
                 Pwd    console ftp snmp  Expires     Attempts  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:ALU-1#
```

Table 33: User field descriptions

Label	Description
User ID	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 Permissions	Console: specifies whether the user is permitted console/Telnet access
	FTP: specifies whether the user is permitted FTP access
	SNMP: specifies whether the user is permitted SNMP access
Password expires	The date on which the current password expires
Attempted logins	The number of times the user has attempted to log in, irrespective of whether the login succeeded or failed
Failed logins	The number of unsuccessful login attempts
Local Conf.	Y: password authentication is based on the local password database
	N: password authentication is not based on the local password database

view

Syntax

view [*view-name*][**detail** | **capabilities**]

Context

show>system>security

Description

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

Parameters

view-name

the name of the view

detail

displays all groups associated with the view

capabilities

displays all views, including excluded MIB-OID trees from unsupported features

Output

The following output is an example of system security view information, and Table 34: System security view field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-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:ALU-1#
```

```
A:ATMIMA1>config# show system security view capabilities
===============================================================================
Views
===============================================================================
view name         oid tree                       mask             permission
-------------------------------------------------------------------------------
iso               1                                                included
iso               1.0.8802                                         no-support
iso               1.3.6.1.3.37                                     no-support
iso               1.3.6.1.3.92                                     no-support
iso               1.3.6.1.3.95                                     no-support
iso               1.3.6.1.2.1.14                                   no-support
iso               1.3.6.1.2.1.15                                   no-support
iso               1.3.6.1.2.1.23                                   no-support
iso               1.3.6.1.2.1.51                                   no-support
iso               1.3.6.1.2.1.68                                   no-support
iso               1.3.6.1.2.1.85                                   no-support
iso               1.3.6.1.2.1.100                                  no-support
iso               1.3.6.1.2.1.4.39                                 no-support
iso               1.3.6.1.2.1.5.20                                 no-support
===============================================================================
A:ALU-1#
```

Table 34: System security view field descriptions

Label	Description
View name	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.
OID tree	The Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.
Mask	The mask value and the mask type, along with the *oid-value* configured in the view command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view
Permission	Included: specifies to include MIB subtree objects
	Excluded: specifies to exclude MIB subtree objects
	No-support: specifies not to support MIB subtree objects
No. of Views	The total number of configured views

Label	Description
Group name	The access group name

5 Event and accounting logs

This chapter provides information about configuring event and accounting logs on the 7705 SAR.

Topics in this chapter include:

- Logging overview
- Log destinations
- Event logs
- Accounting logs
- Configuration notes
- Configuring logging with CLI
- Log command reference

5.1 Logging overview

The two primary types of logging supported on the 7705 SAR are:

- Event logging
- Accounting logs

The log files saved in local storage can be encrypted using the AES-256-CTR algorithm.

Use the following CLI syntax to configure the log file encryption key and enable log file encryption:

```
configure
   log
    encryption-key key [hash | hash2]
```

Note:

- The encrypted log files can be decrypted offline using the appropriate OpenSSL command:

```
openssl enc -aes-256-ctr -pbkdf2 -d -in <log file encrypted> -out <output log file> -p
 -pass pass:<passphrase>
```

- When an encrypted log file is opened in a text editor, editing or viewing the file contents is not possible because the entire file is encrypted.

5.1.1 Event logging

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. Events are messages generated by the system by applications or processes within the 7705 SAR. The 7705 SAR groups events into four major categories or event sources:

- security events – security events are generated by the SECURITY application and pertain to attempts to breach system security
- change events – change events are generated by the USER application and pertain to the configuration and operation of the node
- debug events – debug events are generated by the DEBUG application and pertain to trace or other debugging information
- main events – main events pertain to 7705 SAR applications that are not assigned to other event categories/sources

The applications listed above have the following properties:

- a timestamp 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

Event control assigns the severity for each application event and determines whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7705 SAR conform to ITU standards M.3100 X.733 and X.21 and are listed in the following table.

Table 35: Event severity levels

Severity number	Severity name
1	Cleared
2	Indeterminate (info)
3	Critical
4	Major
5	Minor
6	Warning

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 7705 SAR associates the event sources with logging destinations. Examples of logging destinations include the console 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 are logged in the event log based on combinations of application, severity, event ID range, and the subject of the event.

5.1.2 Accounting logs

The 7705 SAR accounting logs collect comprehensive statistics to support several billing models. The 7705 SAR collects accounting data on services and on network interfaces on a per-forwarding 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 capacity planning. This information is valuable for traffic engineering and capacity planning within the network core.

The 7705 SAR also supports SAA accounting policies.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to customer service access points (SAPs) and network interfaces. Accounting statistics are collected by counters for individual service queues defined on the customer's SAPs 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, which statistics are collected, and the time interval at which to collect statistics.

The only supported destination for an accounting log is a compact flash system device (*cf3*: on all platforms; also *cf1*: or *cf2*: on the 7705 SAR-18). Accounting data is stored within a standard directory structure on the device in compressed XML format.

5.2 Log destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. The 7705 SAR supports the following log destinations:

- Console
- Session
- Memory logs
- Log files
- SNMP trap group
- Syslog

An event log can be associated with multiple event sources, but it can only have a single log destination. Any of the supported log destinations can be configured for an event log.

For an accounting log, the only type of log destination that can be configured is a file destination.

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 that 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 **to session** configuration is removed. Event logs configured with a session destination are stored in the configuration file but the **to session** part of the configuration is not stored. 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 device (*cf3:* on all platforms; also *cf1*: or *cf2*: on the 7705 SAR-18) in the file system. A log file destination is configured using the **config>log>file-id** *log-file-id* command. A log file destination is applied to an event log using the **config>log>log-id>to file** command and to an accounting file using the **config>log>accounting-policy>to file** command.

A log file is identified by a single log file ID, but a log file is generally composed of a number of individual files in the file system. A log file is configured with the following parameters:

- **rollover**: represents the length of time, expressed in minutes, that an individual log file should be written to before a new file is created for the relevant log file ID. The rollover time is checked only when an update to the log is performed. Thus 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.
- **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 retention time is used as a factor to determine which files should be deleted first if the file system device nears 100% usage.

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.

5.2.4.1 Event log files

Event log files are always created in the **\log** directory on the 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, 2015)
– *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)

5.2.4.2 Accounting log files

Accounting log files are created in the `\act-collect` directory on the compact flash device. 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 same form as for event logs.

Accounting logs are **.xml** files that are 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 is 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 (IPv4 or IPv6)
- 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 out-of-band through the Management Ethernet port on the CSM, the source IP address of the trap is the IP interface address defined on the Management Ethernet port. For SNMP traps that will be sent in-band, the source IP address of the trap is the system IP address of the 7705 SAR.

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 (IPv4 or IPv6)
- the UDP port used to send the syslog message
- the Syslog Facility Code
- the Syslog Severity Threshold (0 to 7) (events exceeding the configured level will be sent)

Because syslog uses eight severity levels, whereas the 7705 SAR uses six internal severity levels, the severity levels are mapped to syslog severities. The following table displays the severity level mappings to syslog severities.

Table 36: 7705 SAR-to-syslog severity level mappings

7705 SAR severity level	Syslog severity level (highest to lowest)	Syslog configured severity	Definition
3 critical	0	emergency	System is unusable
	1	alert	Action must be taken immediately
4 major	2	critical	Critical conditions
5 minor	3	error	Error conditions
6 warning	4	warning	Warning conditions
	5	notice	Normal but significant condition
1 cleared	6	info	Informational messages
2 indeterminate	7	debug	Debug-level messages

5.3 Event logs

This section contains the following topics:

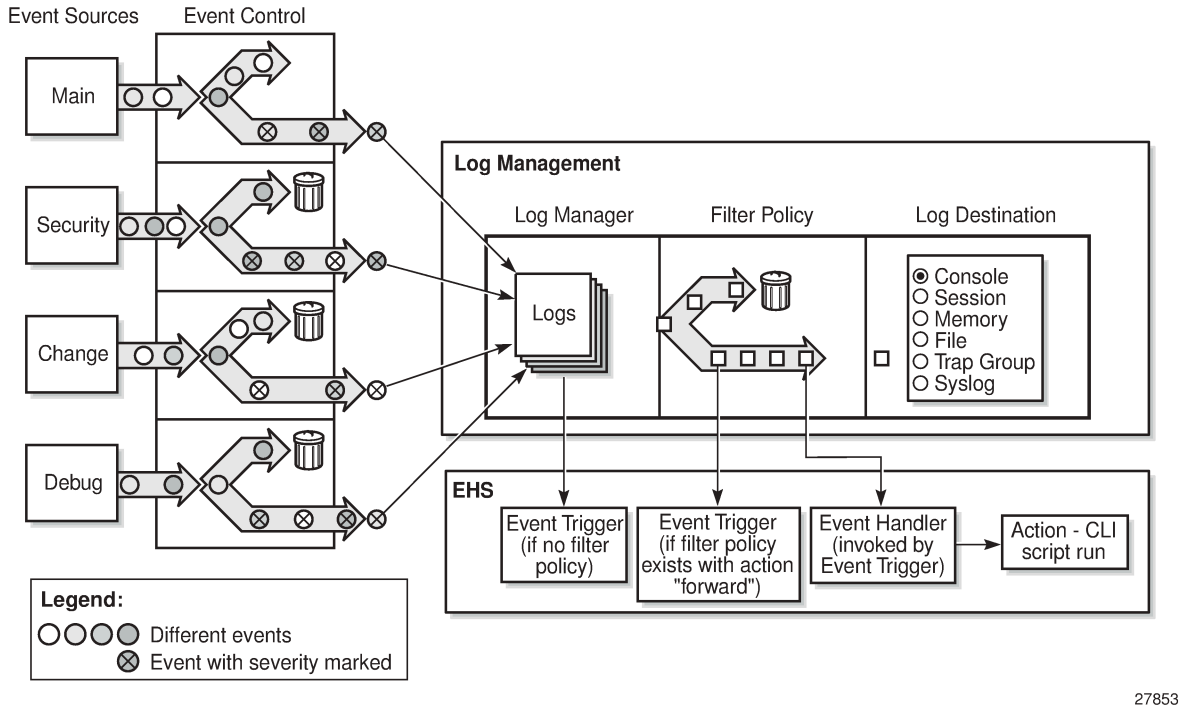
- Event sources
- Event control
- Log manager and event logs
- Event filter policies
- Event log entries
- Simple logger event throttling
- Default system logs

- Event handling system

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 7705 SAR.

The following figure depicts a functional block diagram of event logging.

Figure 4: Event logging block diagram



5.3.1 Event sources

In Figure 4: 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.
- 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.
- 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 7705 SAR

The **show log applications** command displays all applications:

```
*A:ALU-48# show log applications
================================
```

```
Log Event Application Names
==================================
Application Name
----------------------------------
APS
...
BGP
CHASSIS
CPMHWFILTER
...
IGMP_SNOOPING
IP
IPSEC
...
MIRROR
MLD
MLD_SNOOPING
...
ROUTE_POLICY
RSVP
...
VRTR
FIREWALL
...
==================================
*A:ALU-48#
```

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 do not generate log entries as they never reach the log manager.

Simple event throttling is another method of event control and is configured in the same way as 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.

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
-------------------------------------------------------------------------------
ATM:
   2011 tAtmPlcpSubLayerClear            MI  gen          0           0
   2012 tAtmEpOutOfPeerVpiOrVciRange     WA  gen          0           0
   2013 tAtmMaxPeerVccsExceeded          WA  gen          0           0
...
CHASSIS:
   2001 cardFailure                      MA  gen          0           0
```

```
   2002 cardInserted                     MI  gen          7           0
   2003 cardRemoved                      MI  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
FILTER:
   2001 tIPFilterPBRPacketsDrop          WA  gen          0           0
   2002 tFilterEntryActivationFailed     WA  gen          0           0
   2003 tFilterEntryActivationRestored   WA  gen          0           0
GSMP:
   2001 tmnxAncpIngRateMonitorEvent      WA  gen          0           0
L  2002 tmnxAncpIngRateMonitorEventL     WA  gen          0           0
   2003 tmnxAncpEgrRateMonitorEvent      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
...
LDP:
   2001 vRtrLdpStateChange               MI  gen          0           0
   2002 vRtrLdpInstanceStateChange       MI  gen          0           0
   2003 vRtrLdpIfStateChange             MI  gen          0           0
...
LOGGER:
L  2001 STARTED                          MI  gen          5           0
   2002 tmnxLogTraceError                CR  gen          0           0
   2005 tmnxLogSpaceContention           MA  gen          0           0
...
MPLS:
   2001 mplsXCUp                         WA  gen          0           0
   2002 mplsXCDown                       WA  gen          0           0
   2003 mplsTunnelUp                     WA  gen          0           0
...
NTP:
   2001 tmnxNtpAuthMismatch              WA  gen          0           0
   2002 tmnxNtpNoServersAvail            MA  gen          0           0
   2003 tmnxNtpServersAvail              MI  gen          0           0
...
SYSTEM:
   2001 stiDateAndTimeChanged            WA  gen          0           0
   2002 ssiSaveConfigSucceeded           MA  gen          0           0
   2003 ssiSaveConfigFailed              CR  gen          0           0
...
USER:
L  2001 cli_user_login                   MI  gen          4           0
L  2002 cli_user_logout                  MI  gen          3           0
L  2003 cli_user_login_failed            MI  gen          0           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 10 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 control which events are forwarded or dropped based on various criteria. Like other policies with the 7705 SAR, filter policies have a default action. The default actions are either:

- forward
- drop

Filter policies also include a number of filter policy entries that are identified with an entry ID and define specific match criteria and a forward or drop action for the match criteria.

Each entry contains a combination of matching criteria that define the application, event number, router, severity, and subject conditions. The entry's action determines how the packets should be treated if they have met the match criteria.

Entries are evaluated in order from the lowest to the highest entry ID. The first matching event is subject to the forward or drop action for that entry.

Filter policy 1001 exists by default and collects events for the Serious Error Log (log ID 100). Filter policy 1001 is preconfigured with one entry that is configured to collect events of major severity or higher. Filter policy 1001 can be reconfigured by the user.

Valid operators are listed in the following table.

Table 37: Valid filter policy operators

Operator	Description
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

A match criteria entry can include combinations of:

- equal to or not equal to a specified 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 that is appropriate for the specific destination; for example, whether it is to be recorded to a file or sent as an SNMP trap, but log event entries also have common elements or properties. All application-generated events have the following properties:

- a timestamp in UTC or local time
- the generating application
- a unique event ID within the application
- a router name identifying the VRF-ID that generated the event
- a subject identifying the affected object
- a short text description

The general format for an event in an event log with either a memory, console or file destination is as follows:

```
nnnn YYYY/MM/DD HH:MM:SS.SS <severity>:<application> # <event_id> <router-
name> <subject> description
```

The following is an event log example:

```
475 2015/11/27 00:19:40.38 WARNING: SNMP #2008 Base 1/1/1
```

```
"interface 1/1/1 came up"
```

The specific elements that make up the general format are described in the following table.

Table 38: 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* – Day
HH:MM:SS.SS	The UTC timestamp for the event *HH* – Hours (24-hour format) *MM* – Minutes *SS.SS* – Seconds
<severity>	The severity level name of the event CLEARED – a cleared event (severity number 1) INFO – an indeterminate/informational severity event (severity level 2) CRITICAL – a critical severity event (severity level 3) MAJOR – a major severity event (severity level 4) MINOR – a minor severity event (severity level 5) WARNING – a warning severity event (severity 6)
<application>	The application generating the log message
<event_id>	The application's event ID number for the event
<router>	The router name representing the VRF-ID that generated the event
<subject>	The subject/affected object for the event
<description>	A text description of the event

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 application events can be configured to be throttled. When the throttling event limit is exceeded in a throttling interval, any further events of that type are dropped and the dropped events counter is incremented. Dropped events counts are displayed with the **show>log>event-**

control command. 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 that 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. The logger application also cannot distinguish between events that will 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.

By default, event throttling is set to off for each specific event type. It must be explicitly enabled for each event type where throttling is needed. This makes backwards compatibility of configuration files easier to manage.

5.3.7 Default system logs

Log 99 is a preconfigured memory-based log that collects events from the main event source (that is, not the security, debug, or change source). Log 100 is preconfigured to be associated with filter policy 1001, which is preconfigured to collect events of major severity or higher. Log 100 can be reconfigured by the user.

Log 99 and log 100 exist by default.

The following example displays the log 99 and log 100 configurations.

```
ALU-1>config>log# info detail
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
...
        log-id 99
            description "Default system log"
            no filter
            time-format utc
            from main
            to memory 500
            no shutdown
        exit
        log-id 100
           description "Default Serious Errors Log"
           filter 1001
           time-format utc
           from main
           to memory 500
           no shutdown
       exit
----------------------------------------------
```

5.3.8 Event handling system

The event handling system (EHS) is a tool that enables operator-defined behavior to be configured on the 7705 SAR. The operator can define a CLI script that the router executes in response to a log event. The event is referred to as the trigger, where the trigger can be all or part of any event message. Regular expression (regexp) matching can be done on various fields in the log event to give flexibility in the trigger definition.

EHS gives operators the flexibility to configure the 7705 SAR to take actions based on specific events that cannot be done by protocols or services. For example, event-triggered actions can:

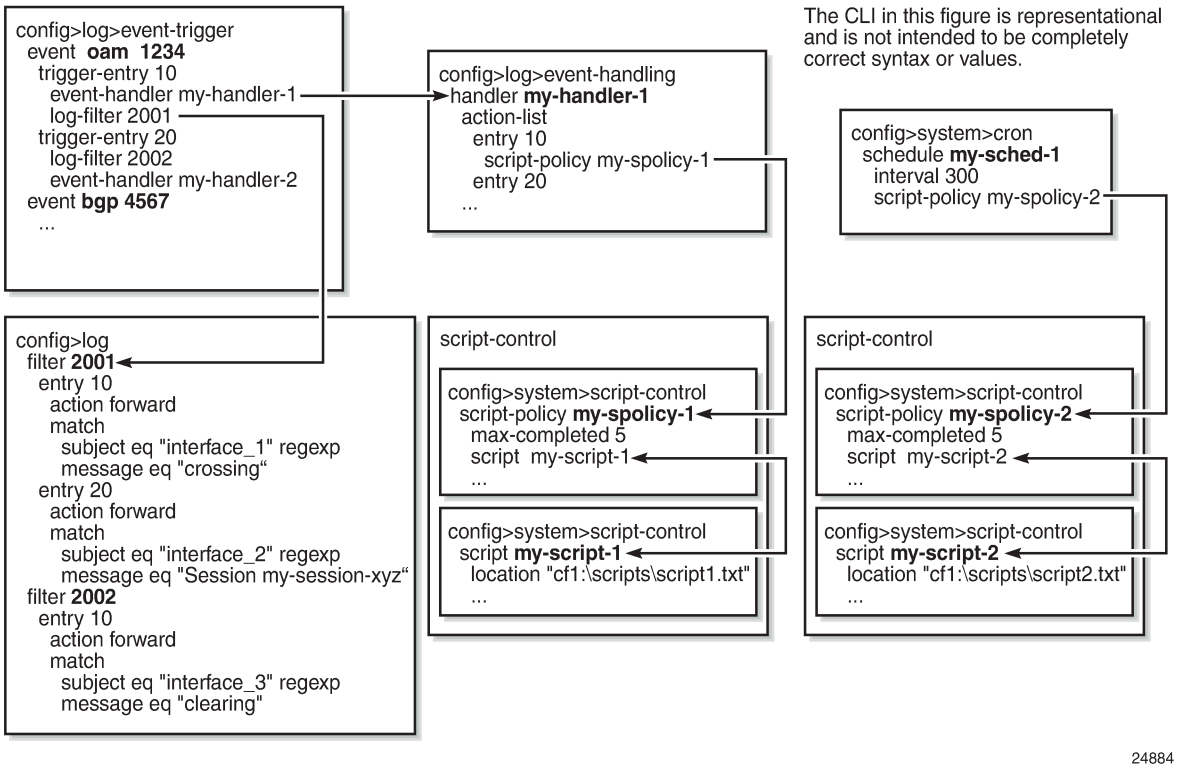
- help with network convergence in response to a specific event
- provide automatic exception handling upon detection of a specific problem

EHS objects are used to tie together trigger events (typically log events that match some configurable criteria) and a set of actions to perform (typically one or more CLI scripts).

EHS, along with CRON, makes use of the **script-control** functions for scripts. Any command available in the CLI can be executed in a script as the result of an event handler being triggered, except for commands that require interaction (for example, a y/n prompt for **admin reboot** without the **now** keyword, or commands that require a password). A script will error out if it encounters a command that requests input.

The following figure shows the relationships between the different configurable objects used by EHS (and CRON).

Figure 5: EHS object relationships



5.3.8.1 Configuring event handling

As shown in Figure 5: EHS object relationships, the steps involved in configuring EHS are:

- configure a script and script policy under the **config>system>script-control** context; the script policy references the configured script
- configure an event handler under the **config>log>event-handling** context and assign actions that reference the previously configured script policy
- configure the event trigger under the **config>log>event-trigger** context that defines the event that triggers the running of the script

See the 7705 SAR Basic System Configuration Guide, "CLI Script Control" for information about configuring scripts and script policies.

5.3.8.1.1 Event handlers

Event handlers are created under the **config>log>event-handling** context. Each event handler is assigned an event handler name and an action list that consists of one or more entries. Each entry in the list references a configured script policy, which in turn references a configured script.

5.3.8.1.2 Event triggers

Event triggers are created under the **config>log>event-trigger** context. Each event trigger is associated with an application and event ID. One or more trigger entries can be configured for the event.

Each trigger entry references a previously configured event handler (which references a configured script policy, which in turn references the script that should be run). A trigger entry can be configured with a previously configured log filter. If a filter is configured, the event trigger calls the filter to determine whether the event should be dropped or forwarded. If the event is to be forwarded, the event trigger invokes the event handler.

All log filter matching options are supported. Regexp matching is supported. Complex rules can be configured to match on log events as a trigger for an EHS event handler.

The EHS triggers on log events that are dropped by user-configured log filters that are assigned to individual logs (with the **config>log>log-id>filter** command). The EHS event trigger occurs before the distribution of log event streams into individual logs.

If there is no filter configured for the trigger entry, the event trigger invokes the event handler as soon as the event occurs.

Log events can be configured to be suppressed or throttled (with the **config>log>event-control** command). EHS does not trigger on suppressed or throttled events.

5.3.8.1.2.1 Debounce

EHS debounce is the ability to trigger an action (for example, an EHS script), if an event happens (N) times within a specific time period (window) in seconds (S):

where:

N = 2 to 15 occurrences

S = 1 to 604800 seconds

For example, if linkDown occurs N times in S seconds, an EHS script is triggered to shut down the port.

Note:

- Triggering happens with the Nth event, not at the end of the time window (S).
- There is no sliding time window (for example, a trigger at the Nth event, N+1 event, and N+2 event) because N is reset after a trigger and the count is restarted.
- When EHS debouncing is used, the varbinds passed in to an EHS script at script triggering time are from the Nth event occurrence (the Nth triggering event); see Variable passing.
- If S is not specified, the 7705 SAR continues to trigger every Nth event.

5.3.8.1.2.2 Variable passing

The common parameters and variable bindings (varbinds) of a triggering log event are passed in to the triggered EHS script and can be used in the script as passed-in (dynamic) variables. These variables are:

- the common event parameters: appid, name, eventid, severity, subject, and gentime
- the predefined varbinds in a log event message; a varbind is a list of values or attributes included in a log event

Passed-in variables are read-only.

Note:

- To view event parameters and varbinds, use the show log event-parameters command.
- The passed-in event **gentime** is always UTC.
- The event sequence number is not passed in to the script.

5.3.8.1.3 EHS scripting

An EHS script can contain local (static) variables and use some basic .if and .set commands. The use of variables with .if and .set commands in an EHS script adds more logic to EHS scripting and allows the reuse of a single EHS script for more than one trigger or action.

Both the passed-in and local variables can be used in the EHS script either as part of the CLI commands or as part of the .if or .set commands.

The following applies to both CLI commands and .if or .set commands:

- Using $X (without using single or double quotes) replaces the variable X with its string or integer value.
- Using "X" (with double quotes) means the literal string X.
- Using "$X" (with double quotes) replaces the variable X with its string or integer value.
- Using 'X' (with single quotes) means the literal string X.
- Using '$X' (with single quotes) does not replace the variable X with its value but means the literal string $X.

In summary:

- All characters within single quotes are interpreted as string characters.

- All characters within double quotes are interpreted as string characters except for $, which replaces the variable with its value (for example, shell expansion inside a string).

Some supported shell command scenarios are as follows (the commands are pseudo commands):

- .if $*string_variable*==*string_value_or_string_variable* {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if ($*string_variable*==*string_value_or_string_variable*) {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if $*integer_variable*==*integer_value_or_integer_variable* {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if ($*integer_variable*==*integer_value_or_integer_variable*) {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if $*string_variable*!=*string_value_or_string_variable* {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if ($*string_variable*!=*string_value_or_string_variable*) {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

  .} endif
- .if $*integer_variable*!=*integer_value_or_integer_variable* {

  CLI_commands_set1

  .} else {

  CLI_commands_set2

.} endif

- .if ($*integer_variable*!=*integer_value_or_integer_variable*) {
  CLI_commands_set1
  .} else {
  CLI_commands_set2
  .} endif
- .set $*string_variable* = *string_value_or_string_variable*
- .set ($*string_variable* = *string_value_or_string_variable*)
- .set $*integer_variable* = *integer_value_or_integer_variable*
- .set ($*integer_variable* = *integer_value_or_integer_variable)*

where:

- *CLI_commands_set1* is a set of one or more CLI commands
- *CLI_commands_set2* is a set of one or more CLI commands
- *string_variable* is a local string variable
- *string_value_or_string_variable* is a string value/variable
- *integer_variable* is a local integer variable
- *integer_value_or_integer_variable* is an integer value/variable

Note:

- A maximum of 100 local variables per EHS script is imposed. Exceeding this limit may result in an error and only partial execution of the script.
- When a set statement is used to set a string_variable to a string_value, the string_value can be any non-integer value with optional single or double quotes.
- A "." preceding a directive (for example, if, and set) is always expected to start a new line.
- An end of line is always expected after {.
- A CLI command is always expected to start a new line.
- Passed-in (dynamic) variables are always read-only inside an EHS script and cannot be overwritten using a set statement.
- .if commands support == and != operators only.
- .if and .set commands support addition, subtraction, multiplication, and division of integers.
- .if and .set commands support concatenation of strings.

Valid examples:

- configure service epipe $serviceID
  where *$serviceID* is either a local integer variable or passed-in integer variable
- echo srcAddr is $srcAddr
  where *$srcAddr* is a passed-in string variable
- .set $ipAddr = "10.0.0.1"

where *$ipAddr* is a local string variable

- .set $ipAddr = $srcAddr
  where *$srcAddr* is a passed-in string variable
  $ipAddr is a local string variable
- .set ($customerID = 50)
  where *$customerID* is a local integer variable
- .set ($totalPackets = $numIngrPackets + $numEgrPackets)
  where *$totalPackets*, *$numIngrPackets*, *$numEgrPackets* are local integer variables
- .set ($portDescription = $portName + $portLocation)
  where *$portDescription*, *$portName*, *$portLocation* are local string variables
- if ($srcAddr == "CONSOLE") {
  CLI_commands_set1
  .else {
  CLI_commands_set2
  .} endif
  where *$srcAddr* is a passed-in string variable
  CLI_commands_set1 is a set of one or more CLI commands
  CLI_commands_set2 is a set of one or more CLI commands
- .if ($customerId == 10) {
  CLI_commands_set1
  .else {
  CLI_commands_set2
  .} endif
  where *$customerID* is a passed-in integer variable
  CLI_commands_set1 is a set of one or more CLI commands
  CLI_commands_set2 is a set of one or more CLI commands
- .if ($numIngrPackets == $numEgrPackets) {
  CLI_commands_set1
  .else {
  CLI_commands_set2
  .} endif
  where *$numIngrPackets* and *$numEgrPackets* are local integer variables
  CLI_commands_set1 is a set of one or more CLI commands
  CLI_commands_set2 is a set of one or more CLI commands

Invalid examples:

- .set $srcAddr = "10.0.0.1"

where *$srcAddr* is a passed-in string variable

Reason: passed-in variables are read-only in an EHS script

- .set ($ipAddr = '$numIngrPackets' + $numEgrPackets)

  where *$ipAddr* is a local string variable

  $numIngrPackets and *$numEgrPackets* are local integer variables

  Reason: variable types do not match; cannot assign a string to an integer
- .set ($numIngrPackets = $ipAddr + $numEgrPackets)

  where *$ipAddr* is a local string variable

  $numIngrPackets and *$numEgrPackets* are local integer variables

  Reason: variable types do not match; cannot concatenate a string to an integer
- .set $ipAddr = "10.0.0.1"100

  where *$ipAddr* is a local string variable

  Reason: when double quotes are used, they must enclose the entire string
- .if ($totalPackets == "10.1.1.1") {

  .} endif

  where *$totalPackets* is a local integer variable

  Reason: cannot compare an integer variable to a string value
- .if ($ipAddr == 10) {

  .} endif

  where *$ipAddr* is a local string variable

  Reason: cannot compare a string variable to an integer value
- .if ($totalPackets == $ipAddr) {

  where *$totalPackets* is a local integer variable

  $ipAddr is a local string variable

  Reason: cannot compare an integer variable to a string variable

5.3.8.1.4 Hardware support

EHS is supported on all 7705 SAR cards, modules, and fixed platforms.

5.4 Accounting logs

This section contains the following topics:

- Accounting records
- Accounting files
- Design considerations

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 a compact flash (*cf3*: on all platforms; also *cf1*: or *cf2*: on the 7705 SAR-18) in a compressed (tar) XML format and can be retrieved using FTP or SCP.

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 following table lists the record name, sub-record types, and default collection period for service and network accounting policies.

Table 39: Accounting record name and collection periods

Record name	Sub-record types	Accounting object	Default collection period (minutes)
service-ingress-octets	sio	SAP	5
service-egress-octets	seo	SAP	5
service-ingress-packets	sip	SAP	5
service-egress-packets	sep	SAP	5
combined-service-ing-egr-octets	cmSio and cmSeo	SAP	5
complete-service-ingress-egress	cpSipo and cpSepo	SAP	5
saa	saa (png) trc hop	SAA or SAA test	5
network-ingress-octets	nio	Network port	15
network-egress-octets	neo	Network port	15
network-ingress-packets	nip	Network port	15
network-egress-packets	nep	Network port	15
combined-network-ing-egr-octets	cmNio and cmNeo	Network port	15
complete-network-ingr-egr	cpNipo and cpNepo	Network port	15
combined-mpls-lsp-ingress combined-mpls-lsp-egress	mplsLspIng mplsLspEg	lsp	5

Record name	Sub-record types	Accounting object	Default collection period (minutes)
combined-ldp-lsp-egress	ldpEgr	lsp	5

The 7705 SAR supports simultaneous collection for some records. For example, "complete-network-ingr-egr" (cpNipo and cpNepo) simultaneously collects statistics on network-ingress octets, network-ingress packets, network-egress octets, and network-egress packets for the same network port.

Similarly, on the service side, "complete-service-ingr-egr" (cpSipo and cpSepo) simultaneously collects statistics on service-ingress octets, service-ingress packets, service-egress octets, and service-egress packets from a single SAP.

When creating accounting policies, one service accounting policy and one network accounting policy can be defined as the default. If statistics collection is enabled on a SAP or network port and no accounting policy is applied, the respective default policy is used. If no default policy is 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, which are in turn composed of multiple fields. The following table lists the accounting policy record names and the statistics that are collected with each.

Table 40: Accounting record name details

Record name	Sub-record	Field	Field description
combined-mpls-lsp-ingress combined-mpls-lsp-egress combined-ldp-lsp-egress	cmmplslspi cmmplslspe cmldplspe	cmmplslspi	combined mpls lsp ingress
		cmmplslspe	combined mpls lsp egress
		cmldplspe	combined ldp lsp egress
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ipf	In-profile packets forwarded
		opf	Out-of-profile packets forwarded
		fc	Packet forwarding class
service-ingress-octets	sio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped

Record name	Sub-record	Field	Field description
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
service-egress-octets	seo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
service-ingress-packets	sip	svc	SvcId
		sap	SapId
		qid	QueueId
		hpo	HighPktsOffered
		hpd	HighPktsDropped
		lpo	LowPktsOffered
		lpd	LowPktsDropped
		ucp	UncoloredPacketsOffered
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
service-egress-packets	sep	svc	SvcId
		sap	SapId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped

Record name	Sub-record	Field	Field description
		sap	SapId
		slaProfile	SlaProfile
complete-service-ingress-egress (cp Sipo and cpSepo)	cpSipo	svc	SvcId
		sap	SapId
		pid	PolicerId
		hpo	HighPktsOffered
		hpd	HighPktsDropped
		lpo	LowPktsOffered
		lpd	LowPktsDropped
		ucp	UncoloredPacketsOffered
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		apo	AllPacketsOffered
		aoo	AllOctetsOffered
		apd	AllPacketsDropped
		aod	AllOctetsDropped
		apf	AllPacketsForwarded
		aof	AllOctetsForwarded
		ipd	InProfilePktsDropped
		iod	InProfileOctetsDropped
		opd	OutOfProfilePktsDropped
		ood	OutOfProfileOctetsDropped
		hpf	HighPriorityPacketsForwarded
		hof	HighPriorityOctetsForwarded

Record name	Sub-record	Field	Field description
		lpf	LowPriorityPacketsForwarded
		lof	LowPriorityOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
	cpSepo	svc	SvcId
		sap	SapId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
combined-service-ingr-egr-octets (cmSio and CmSeo)	cmSio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded

Record name	Sub-record	Field	Field description
	cmSeo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
network-ingress-octets	nio	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
network-egress-octets	neo	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
network-ingress-packets	nip	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
network-egress-packets	nep	port	PortId
		qid	QueueId

Record name	Sub-record	Field	Field description
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
combined-network-ing-egr-octets (cmNio and cmNeo)	cmNio	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
	cmNeo	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
complete-network-ingr-egr (cpNipo and cpNepo)	cpNipo	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
	cpNepo	port	PortId

Record name	Sub-record	Field	Field description
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
saa	saa	tmd	TestMode
		own	OwnerName
		tst	TestName
		png	PingRun subrecord
		rid	RunIndex
		trr	TestRunResult
		mnr	MinRtt
		mxr	MaxRtt
		avr	AverageRtt
		rss	RttSumOfSquares
		pbr	ProbeResponses
		spb	SentProbes
		mnt	MinOutTt
		mxt	MaxOutTt
		avt	AverageOutTt
		tss	OutTtSumOfSquares
		mni	MinInTt
		mxi	MaxInTt

Record name	Sub-record	Field	Field description
		avi	AverageInTt
		iss	InTtSumOfSqrs
		ojt	OutJitter
		ijt	InJitter
		rjt	RtJitter
		prt	ProbeTimeouts
		prf	ProbeFailures
	trc	rid	RunIndex
		trr	TestRunResult
		lgp	LastGoodProbe
	hop	hop	TraceHop
		hid	HopIndex
		mnr	MinRtt
		mxr	MaxRtt
		avr	AverageRtt
		rss	RttSumOfSquares
		pbr	ProbeResponses
		spb	SentProbes
		mnt	MinOutTt
		mxt	MaxOutTt
		avt	AverageOutTt
		tss	OutTtSumOfSquares
		mni	MinInTt
		mxi	MaxInTt
		avi	AverageInTt
		iss	InTtSumOfSqrs
		ojt	OutJitter

Record name	Sub-record	Field	Field description
		ijt	InJitter
		rjt	RtJitter
		prt	ProbeTimeouts
		prf	ProbeFailures
		tat	TraceAddressType
		tav	TraceAddressValue

5.4.2 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 7705 SAR creates two directories on the compact flash to store the files. The following output displays a directory named `act-collect` that holds accounting files that are open and actively collecting statistics, and a directory named `act` that stores the files that have been closed and are awaiting retrieval.

```
ALU-1>file cf3:\# dir act*
12/19/2006 06:08a      <DIR>          act-collect
12/19/2006 06:08a      <DIR>          act

ALU-1>file cf3:\act-collect\ # dir
Directory of cf3:\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 (such as rollover and retention) are discussed in more detail in Log files.

A file ID can only be assigned to either one event log ID or one accounting log.

5.4.3 Design considerations

The 7705 SAR has ample resources to support large-scale accounting policy deployments. 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 and network interfaces 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 are logging configuration guidelines and 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 in the **config>log** context 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.
- A log ID associated with the **snmp-trap-group** command must be the same as a log ID associated with the **log-id** command.

5.6 Configuring logging with CLI

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

Topics in this section include:

- Log configuration overview
- Log type
- Basic event log configuration
- Common configuration tasks
- Log management tasks

5.7 Log configuration overview

Logging on the 7705 SAR is used to provide the operator with logging information for monitoring and troubleshooting. You can configure logging parameters to save information in a log file or direct the messages to other devices. Logging commands allow you to:

- select the types of logging information to be recorded
- assign a severity to the log messages
- select the source and target of logging information

5.8 Log type

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 that identify targets to send traps following specified events
- syslog – information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element
- event control – configures a particular event, or all events associated with an application, to be generated or suppressed
- event filters – an event filter defines whether to forward or drop an event or trap based on match criteria
- accounting policies – an accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more service access points (SAPs) and to network ports.
- event logs – an event log defines the types of events to be delivered to an associated destination
- event throttling rate – defines the rate of throttling events

5.9 Basic event log configuration

The most basic log configuration must have the following:

- a log ID or an accounting policy ID
- a log source
- a log destination

The following displays a log configuration example.

```
ALU-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        file-id 1
            description "This is a test file-id."
            location cf3:
        exit
        file-id 2
            description "This is a test log."
            location cf3:
        exit
        snmp-trap-group 7
            trap-target 10.10.10.10 "snmpv2c" notify-community "public"
        exit
        log-id 2
            from main
            to file 2
        exit
----------------------------------------------
ALU-12>config>log#
```

5.10 Common configuration tasks

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

- Configuring an event log
- Configuring a file ID
- Configuring an accounting policy
- Configuring event control and throttle rate
- Configuring a log filter
- Configuring an SNMP trap group
- Configuring a syslog target

5.10.1 Configuring an event log

An event log file is identified by a *log-id* and contains information used to direct messages generated by system applications (such as events, alarms, traps, and debug information) to their respective destinations. One or more event sources can be specified using the **from** command. Event destinations (such as file IDs, SNMP trap groups, or syslog IDs) must be configured using the **to** command before they can be applied to an event log ID. Only one destination can be specified.

Use the **file-id** *log-file-id* command to specify the destination compact flash. See Configuring a file ID.

Use the following CLI syntax to configure a log file:

CLI syntax:

```
config>log
    log-id log-id
        description description-string
        filter filter-id
        from {[main] [security] [change] [debug-trace]}
        to console
        to file log-file-id
        to memory [size]
        to session
        to snmp [size]
        to syslog syslog-id
        time-format {local | utc}
        no shutdown
```

The following displays an example of the event log file configuration command syntax:

Example:

```
config# log
config>log# log-id 2
config>log>log-id$ description "This is a test log file."
config>log>log-id# filter 1
config>log>log-id# from main security
config>log>log-id# to file 1
config>log>log-id# no shutdown
config>log>log-id# exit
```

The following displays a log file configuration:

```
ALU-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
...
-----------------------------------------------
ALU-12>config>log>log-id#
```

5.10.2 Configuring a file ID

To create a log file, a file ID is defined that specifies the target compact flash drive and the rollover and retention interval period for the file. The rollover interval is defined in minutes and determines how long a file is used before it is closed and a new log file is created. The retention interval determines how long the file is stored on the compact flash drive before it is deleted.

The minimum amount of free space for log files on a compact flash drive is the lesser of 10% of the compact flash disk capacity or 5 Mb (5 242 880).

Use the following CLI syntax to configure a log file ID:

CLI syntax:

```
config>log
    file-id log-file-id
        description description-string
        location cflash-id
        rollover minutes[retention hours]
```

The following displays an example of the log file ID configuration command syntax:

Example:

```
config# log
config>log# file-id 1
config>log>file-id# description "This is a log file."
config>log>file-id# location cf3:
config>log>file-id# rollover 600 retention 24
```

The following displays the file ID configuration:

```
ALU-12>config>log# info
----------------------------------------
        file-id 1
            description "This is a log file."
            location cf3:
            rollover 600 retention 24
        exit
----------------------------------------------
ALU-12>config>log#
```

5.10.3 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 on the compact flash drive 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 SAP or service interface, or applied to a network port. For information about associating an accounting policy with a SAP or a network port, see the 7705 SAR Services Guide or the 7705 SAR Interface Configuration Guide (respectively).

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 service accounting policy and one network accounting policy can be defined as **default**. If statistics collection is enabled on a SAP or network port and no accounting policy is applied, the respective default policy is used. If no default policy is defined, no statistics are collected unless a specifically defined accounting policy is applied.

Use the following CLI syntax to configure an accounting policy:

CLI syntax:

```
config>log>
    accounting-policy acct-policy-id
        collection-interval minutes
        default
        description description-string
        record record-name
        to file log-file-id
        no shutdown
```

The following displays an example of the accounting policy configuration command syntax:

Example:

```
config>log# accounting-policy 4
config>log>acct-policy# description "This is the default
  accounting policy."
config>log>acct-policy# record service-ingress-packets
config>log>acct-policy# default
config>log>acct-policy# to file 1
config>log>acct-policy# exit
config>log# accounting-policy 5
config>log>acct-policy# description "This is a test
  accounting policy."
config>log>acct-policy# record service-ingress-packets
config>log>acct-policy# to file 2
config>log>acct-policy#
```

The following displays the accounting policy configuration:

```
ALU-12>config>log# info
----------------------------------------------
    accounting-policy 4
        description "This is the default accounting policy."
        record service-ingress-packets
        default
        to file 1
    exit
    accounting-policy 5
        description "This is a test accounting policy."
        record service-ingress-packets
        to file 2
    exit
----------------------------------------------
ALU-12>config>log#
```

5.10.4 Configuring event control and throttle rate

Use the following CLI syntax to configure event control. 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. The throttling rate can also be configured independently for each log event by using the **specific-throttle-rate** parameter; this rate overrides the globally configured throttle rate for the specified log event.

CLI syntax:

```
config>log
    event-control application-id [event-name | event-number] generate
 [severity-level][throttle] [specific-throttle-rate events-limit
 interval seconds | disable-specific-throttle]
    event-control application-id [event-name |event-number] suppress
    throttle-rate events[interval seconds]
```

The following displays an example of throttle rate configuration for all events that have throttling enabled:

Example:

```
config# log
config>log# event-control aps 2003 generate major throttle
config>log# event-control aps 2006 generate major throttle
config>log# throttle-rate 500 interval 10
```

The following displays the throttle rate configuration:

```
ALU-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        throttle-rate 500 interval 10
        event-control "aps" 2003 generate major throttle
        event-control "aps" 2006 generate major throttle
..
--------------------------------------------
ALU-12>config>log>#
```

The following displays an example of throttle rate configuration for a specific event. The **specific-throttle-rate** configured for application **aps**, event **2003**, overrides the globally configured **throttle-rate**.

Example:

```
config# log
config>log# event-control aps 2003 generate major throttle specific-
throttle-rate 600 interval 15
config>log# event-control aps 2006 generate major throttle
config>log# throttle-rate 500 interval 10
```

The following displays the specific throttle rate configuration:

```
ALU-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        throttle-rate 500 interval 10
        event-control "aps" 2003 generate major throttle specific-throttle-
rate 600 interval 15
```

```
        event-control "aps" 2006 generate major throttle
..
-----------------------------------------------
ALU-12>config>log>#
```

5.10.5 Configuring a log filter

Use the following CLI syntax to configure a log filter:

CLI syntax:

```
config>log
    filter filter-id
        default-action {drop | forward}
        description description-string
        entry entry-id
            action {drop | forward}
            description description-string
            match
                application {eq | neq} application-id
                message {eq | neq} pattern pattern [regexp]
                number {eq | neq | lt | lte | gt | gte} event-id
                router {eq | neq} router-instance [regexp]
                severity {eq | neq | lt | lte | gt | gte} severity-
level
                subject {eq | neq} subject [regexp]
```

The following displays an example of the log filter configuration command syntax:

Example:

```
config# log
config>log# filter 1
config>log>filter# description "This is a test filter."
config>log>filter# default-action drop
config>log>filter# entry 1
config>log>filter>entry$ action forward
config>log>filter>entry# match application eq atm
config>log>filter>entry# match severity eq critical
config>log>filter>entry# exit
```

The following displays the log filter configuration:

```
ALU-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        file-id 1
            description "This is our log file."
            location cf3:
            rollover 600 retention 24
        exit
        filter 1
            default-action drop
            description "This is a test filter."
            entry 1
                action forward
                match
                    application eq "atm"
                    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
...
-----------------------------------------
ALU-12>config>log#
```

5.10.6 Configuring an SNMP trap group

The associated *log-id* does not have to be configured before a **snmp-trap-group** can be created; however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

Use the following CLI syntax to configure an SNMP trap group:

CLI syntax:

```
config>log
    snmp-trap-group log-id
        trap-target name address ip-address [port port] [snmpv1 |
 snmpv2c | snmpv3] notify-community communityName|snmpv3Security
Name[security-level {no-auth-no-privacy |
        auth-no-privacy | privacy}]
```

The following displays an example of the SNMP trap group configuration command syntax:

Example:

```
config# log
config>log# snmp-trap-group 2
config>log>snmp-trap-group# trap-target "target name" address
 10.10.10.104  notify-community "communitystring" security-level  no-
auth-no-privacy
config>log>snmp-trap-group# exit
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
    snmp-trap-group 2
        trap-target "target name" address 10.10.10.104:5 "snmpv3" notify-community
         "communitystring"
        exit
...
    log-id 2
            description "This is a test log file."
            filter 1
            from main security
            to file 1
    exit
...
----------------------------------------------
ALU-12>config>log#
```

5.10.7 Configuring a syslog target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

Use the following CLI syntax to configure a syslog file:

CLI syntax:

```
config>log
    syslog syslog-id
        address ip-address
        description description-string
        facility syslog-facility
        level {emergency | alert | critical | error | warning | notice
 | info | debug}
        log-prefix log-prefix-string
        port port
```

The following displays an example of the syslog file configuration command syntax:

Example:

```
config# log
config>log# syslog 1
config>log>syslog$ description "This is a syslog file."
config>log>syslog# address 10.10.10.104
config>log>syslog# facility user
config>log>syslog# level warning
```

The following displays the syslog configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "This is a syslog file."
            address 10.10.10.104
            facility user
            level warning
        exit
...
----------------------------------------------
ALU-12>config>log#
```

5.11 Log management tasks

This section discusses the following logging tasks:

- Modifying a log file
- Deleting a log file
- Modifying a file ID
- Deleting a file ID
- Modifying a syslog ID
- Deleting a syslog ID

- Modifying an SNMP trap group
- Deleting an SNMP trap group
- Modifying a log filter
- Deleting a log filter
- Modifying event control parameters
- Returning to the default event control configuration

5.11.1 Modifying a log file

If the log destination needs to be changed or if the *size* of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Use the following CLI syntax to modify a log file:

CLI syntax:

```
config>log
    log-id log-id
        description description-string
        filter filter-id
        from {[main] [security] [change] [debug-trace]}
        to console
        to file file-id
        to memory [size]
        to session
        to snmp [size]
        to syslog syslog-id
```

The following displays the current log configuration:

```
ALU-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
...
----------------------------------------------
ALU-12>config>log>log-id#
```

The following displays an example of modifying log file parameters:

Example:

```
config# log
config>log# log-id 2
config>log>log-id# description "Chassis log file."
config>log>log-id# filter 2
config>log>log-id# from security
config>log>log-id# exit
```

The following displays the modified log file configuration:

```
ALU-12>config>log# info
```

```
-----------------------------------------------
...
    log-id 2
            description "Chassis log file."
            filter 2
            from security
            to file 1
    exit
...
-----------------------------------------------
ALU-12>config>log#
```

5.11.2 Deleting a log file

The log ID must be shut down first before it can be deleted. In a previous example, file 1 is associated with **log-id 2**.

```
ALU-12>config>log# info
-----------------------------------------------
    file-id 1
            description "LocationTest."
            location cf3:
            rollover 600 retention 24
        exit
...
    log-id 2
            description "Chassis log file."
            filter 2
            from security
            to file 1
    exit
...
-----------------------------------------------
ALU-12>config>log#
```

Use the following CLI syntax to delete a log file:

CLI syntax:

```
config>log
    no log-id log-id
        shutdown
```

The following displays an example of deleting a log file:

Example:

```
config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

5.11.3 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 is not cleared, the old location remains in effect.

Use the following CLI syntax to modify a file ID:

CLI syntax:

```
config>log
    file-id log-file-id
        description description-string
        location [cflash-id]
        rollover minutes[retention hours]
```

The following displays the current file ID configuration:

```
ALU-12>config>log# info
----------------------------------------
        file-id 1
            description "This is a log file."
            location cf3:
            rollover 600 retention 24
        exit
----------------------------------------------
ALU-12>config>log#
```

The following displays an example of modifying file ID parameters:

Example:

```
config# log
 config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# location cf3:
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file ID modifications:

```
ALU-12>config>log# info
----------------------------------------------
...
   file-id 1
            description "LocationTest."
            location cf3:
            rollover 2880 retention 500
        exit
...
----------------------------------------------
```

5.11.4 Deleting a file ID

Note: All references to the file ID must be deleted before the file ID can be removed.

Use the following CLI syntax to delete a file ID:

CLI syntax:

```
config>log
```

```
    no file-id log-file-id
```

The following displays an example of deleting a file ID:

Example:

```
config>log# no file-id 1
```

5.11.5 Modifying a syslog ID

Use the following CLI syntax to modify syslog ID parameters:

CLI syntax:

```
config>log
    syslog syslog-id
        address ip-address
        description description-string
        facility syslog-facility
        level {emergency | alert | critical | error | warning | notice
 | info | debug}
        log-prefix log-prefix-string
        port port
```

The following displays an example of the syslog ID modifications:

Example:

```
config# log
config>log# syslog 1
config>log>syslog$ description "Test syslog."
config>log>syslog# address 10.10.0.91
config>log>syslog# facility mail
config>log>syslog# level info
```

The following displays the syslog configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "Test syslog."
            address 10.10.10.91
            facility mail
            level info
        exit
...
----------------------------------------------
ALU-12>config>log#
```

5.11.6 Deleting a syslog ID

Note: All references to the syslog ID must be deleted before the syslog ID can be removed. Use the **show>log>log-id** command to view syslog references.

Use the following CLI syntax to delete a syslog ID:

CLI syntax:

```
config>log
    no syslog syslog-id
```

The following displays an example of deleting a syslog ID:

Example:

```
config# log
config>log# no syslog 1
```

5.11.7 Modifying an SNMP trap group

Use the following CLI syntax to modify an SNMP trap group:

CLI syntax:

```
config>log
    snmp-trap-group log-id
        trap-target name [address ip-address] [port port] [snmpv1
 | snmpv2c | snmpv3] notify-community communityName|snmpv3Security
Name[security-level {no-auth-no-privacy |
auth-no-privacy | privacy}]
```

The following displays the current SNMP trap group configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
    snmp-trap-group 10
        trap-target 10.10.10.104:5 "snmpv3" notify-community "communitystring"
    exit
...
----------------------------------------------
ALU-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

Example:

```
config# log
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.10.104:5
config>log>snmp-trap-group# snmp-trap-group#  trap- target
 10.10.0.91:1 snmpv2c notify-community "com1"
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
        snmp-trap-group 10
            trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
        exit
...
----------------------------------------------
ALU-12>config>log#
```

5.11.8 Deleting an SNMP trap group

Use the following CLI syntax to delete a trap target and SNMP trap group:

CLI syntax:

```
config>log
    no snmp-trap-group log-id
        no trap-target name
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
       snmp-trap-group 10
           trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
       exit
...
----------------------------------------------
ALU-12>config>log#
```

The following displays an example of deleting a trap target and an SNMP trap group.

Example:

```
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.0.91:1
config>log>snmp-trap-group# exit
config>log# no snmp-trap-group 10
```

5.11.9 Modifying a log filter

Use the following CLI syntax to modify a log filter:

CLI syntax:

```
config>log
    filter filter-id
        default-action {drop | forward}
        description description-string
        entry entry-id
            action {drop | forward}
            description description-string
            match
                application {eq | neq} application-id
                message {eq | neq} pattern pattern [regexp]
                number{eq | neq | lt | lte | gt | gte}event-id
                router {eq | neq} router-instance [regexp]
                severity {eq | neq | lt | lte | gt | gte} severity-
level
                subject {eq | neq} subject [regexp]
```

The following output displays the current log filter configuration:

```
ALU-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
```

```
...
        filter 1
            default-action drop
            description "This is a test filter."
            entry 1
                action forward
                match
                    application eq "atm"
                    severity eq critical
                exit
            exit
        exit
...
----------------------------------------
ALU-12>config>log#
```

The following displays an example of the log filter modifications:

Example:

```
config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
ALU-12>config>log>filter# info
----------------------------------------
...
            description "This allows <n>."
            entry 1
                action drop
                match
                    application eq "user"
                    number eq 2001
                exit
            exit
        exit
...
----------------------------------------
ALU-12>config>log>filter#
```

5.11.10 Deleting a log filter

Use the following CLI syntax to delete a log filter:

CLI syntax:

```
config>log
    no filter filter-id
```

The following displays an example of the command to delete a log filter:

Example:

```
config>log# no filter 1
```

5.11.11 Modifying event control parameters

Use the following CLI syntax to modify event control parameters:

CLI syntax:

```
config>log
    event-control application-id [event-name | event-number] generate
 [severity-level][throttle] [specific-throttle-rate events-limit
 interval seconds | disable-specific-throttle]
    event-control application-id [event-name |event-number] suppress
```

The following displays the current event control configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
    event-control "atm" 2014 generate critical
...
----------------------------------------------
ALU-12>config>log#
```

The following displays an example of event control modifications:

Example:

```
config# log
config>log# event-control atm 2014 suppress
```

The following displays the log filter configuration:

```
ALU-12>config>log# info
----------------------------------------------
...
        event-control "atm" 2014 suppress
...
----------------------------------------------
ALU-12>config>log#
```

5.11.12 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 CLI syntax to return to the default event control configuration:

CLI syntax:

```
config>log
    no event-control application [event-name |event-number]
```

The following displays an example of the command usage to return to the default values:

Example:

```
config# log
config>log# no event-control "atm" 2014
config>log# no event-control "filter" 2001
config>log# no event-control "mpls" 2001
```

```
ALU-12>config>log# info detail
----------------------------------------------
#----------------------------------------
echo "Log Configuration"
#----------------------------------------
...
        event-control "atm" 2004 generate minor
        event-control "atm" 2005 generate warning
        event-control "atm" 2006 generate warning
        event-control "atm" 2007 generate critical
        event-control "atm" 2008 generate warning
        event-control "atm" 2009 generate warning
        event-control "atm" 2010 generate warning
        event-control "atm" 2011 generate warning
        event-control "atm" 2012 generate warning
        event-control "atm" 2013 generate warning
        event-control "atm" 2014 generate warning
        event-control "atm" 2015 generate warning
        event-control "atm" 2016 generate warning
        event-control "atm" 2017 generate warning
...
----------------------------------------------
ALU-12>config>log#
```

5.12 Log command reference

5.12.1 Command hierarchies

- Configuration commands
  - Accounting policy commands
  - Event control commands
  - Event handling commands
  - Event trigger commands
  - Log file commands
  - Log filter commands
  - Syslog commands
  - Logging destination commands
  - SNMP trap group commands
- Show commands
- Clear commands

5.12.1.1 Configuration commands

5.12.1.1.1 Accounting policy commands

```
config
- log
        - accounting-policy acct-policy-id
        - no accounting-policy acct-policy-id
            - collection-interval minutes
            - no collection-interval
            - [no] default
            - description description-string
            - no description
            - record record-name
            - no record
            - [no] shutdown
            - to file log-file-id
            - to no-file
```

5.12.1.1.2 Event control commands

```
config
- log
        - event-control application-id [event-name | event-number] generate [severity-level]
 [throttle] [specific-throttle-rate events-limit interval seconds | disable-specific-throttle]
        - event-control application-id [event-name | event-number] suppress
```

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

5.12.1.1.3 Event handling commands

```
config
- log
        - event-handling
            - [no] handler event-handler-name
                - action-list
                    - [no] entry entry-id
                        - description description-string
                        - no description
                        - min-delay [delay]
                        - no min-delay
                        - script-policy policy-name [owner policy-owner]
                        - no script-policy
                        - [no] shutdown
                - description description-string
                - no description
                - [no] shutdown
```

5.12.1.1.4 Event trigger commands

```
config
- log
        - event-trigger
            - [no] event application-id event-name-id
                - description description-string
                - no description
                - [no] shutdown
                - [no] trigger-entry entry-id
                    - debounce occurrences [within seconds]
                    - no debounce
                    - description description-string
                    - no description
                    - event-handler event-handler
                    - no event-handler
                    - log-filter filter-id
                    - no log-filter
                    - [no] shutdown
```

5.12.1.1.5 Log file commands

```
config
- log
        - encryption-key key [hash | hash2]
        - no encryption-key
        - [no] file-id log-file-id
            - description description-string
            - no description
            - location cflash-id
            - rollover minutes [retention hours]
            - no rollover
```

5.12.1.1.6 Log 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
                    - message {eq | neq} pattern pattern [regexp]
                    - no message
                    - 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
```

5.12.1.1.7 Syslog commands

```
config
- log
        - [no] syslog syslog-id
            - address ip-address
            - no address
            - description description-string
            - no description
            - facility syslog-facility
            - no facility
            - level syslog-level
            - no level
            - log-prefix log-prefix-string
            - no log-prefix
            - port port
            - no port
```

5.12.1.1.8 Logging destination 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
```

5.12.1.1.9 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}]
            - no trap-target name
```

5.12.1.2 Show commands

```
show
- log
        - accounting-policy [acct-policy-id] [access | network] [associations]
        - accounting-records
        - applications
        - event-control [application-id [event-name | event-number]]
        - event-control application-id event-name detail
        - event-handling
            - handler [handler-name]
            - handler detail
            - information
            - scripts
        - event-parameters [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]
```

5.12.1.3 Clear commands

```
clear
- log
        - log-id log-id
        - event-handling
            - handler  event-handler-name
            - information
```

5.12.2 Command descriptions

- Configuration commands
- Show commands
- Clear commands

5.12.2.1 Configuration commands

- Generic commands
- Accounting policy commands
- Event control commands
- Event handling commands
- Event trigger commands
- Log file commands
- Log filter commands
- Syslog commands
- Logging destination commands
- SNMP trap group commands

5.12.2.1.1 Generic commands

description

Syntax

description *description-string*

no description

Context

config>log>accounting-policy

config>log>event-handling>handler

config>log>event-handling>handler>action-list>entry

config>log>event-trigger>event

config>log>event-trigger>event>trigger-entry

config>log>file-id

config>log>snmp-trap-group

config>log>filter

config>log>filter>entry

config>log>log-id

config>log>syslog

Description

This command creates a text description stored in the configuration file for a configuration context.

The command associates a text string with a configuration context to help identify the content in the configuration file.

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

Default

No text description is associated with this configuration.

Parameters

string

The description can contain a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (such as #, $, or spaces), the entire string must be enclosed within double quotes.

shutdown

Syntax

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

Context

config>log>accounting-policy

config>log>event-handling>handler

config>log>event-handling>handler>action-list>entry

config>log>event-trigger>event

config>log>event-trigger>event>trigger-entry

config>log>log-id

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 can 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.

5.12.2.1.2 Accounting policy commands

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy *acct-policy-id*

Context

config>log

Description

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

Access accounting policies are policies that can be applied to one or more service access points (SAPs). Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.

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

If an accounting policy is not specified on a SAP or network port, accounting records are produced in accordance with the access or network policy designated as the **default**. For more information, see the default command.

The **no** form of the command deletes the policy from the configuration. The accounting policy cannot be deleted unless it is removed from all the SAPs or network ports where the policy is applied. Use the **show>log>accounting-policy** command to see where an accounting policy is used and which accounting policy is the default policy.

Default

n/a

Parameters

acct-policy-id

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

Description

This command configures the interval between collection of accounting records.

Parameters

minutes

the interval, in minutes, at which accounting records are collected

Values 1 to 120

default

Syntax

[**no**] **default**

Context

config>log>accounting-policy

Description

This command configures the accounting policy specified by *acct-policy-id* to be the default accounting policy that is used by all SAPs or network ports that do not have a specified accounting policy.

For a SAP or network port, if no accounting policy is explicitly specified and a **default** policy is defined, records are produced as per the **default** accounting policy. If no **default** policy is defined, no records are collected. However, if an accounting policy is explicitly defined for a SAP or network port, records are collected for that SAP or network port.

Only one access accounting policy ID can be designated as the default access policy. Similarly, only one network accounting policy ID can be designated as the default network accounting policy.

The *record-name* must be specified before configuring an accounting policy as **default**.

If a policy is configured as the default policy, a **no default** command must be issued before a new default policy can be configured.

Default accounting policies cannot be explicitly applied. For example, if **default** is set for **accounting-policy 10**, policy 10 cannot be assigned.

The **no** form of the command removes the default pol icy designation from the policy ID. The accounting policy is removed from all SAPs or network ports that do not have a policy explicitly defined. If there is no policy defined as the **default** policy, no accounting policy is applied to those entities.

record

Syntax

record *record-name*

no record

Context

config>log>accounting-policy

Description

This command adds the record name to the accounting policy, specifying which records to forward to the configured accounting file (identified by *log-file-id*). Each accounting policy can only contain one record name. To obtain a list of all record types that can be configured, use the **show>log>accounting-records** command.

```
ALU-12>config>log# 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
11       combined-network-ing-egr-octets   15
12       combined-service-ing-egr-octets   5
13       complete-service-ingress-egress   5
32       saa                               5
54       complete-network-ing-egr          15
===========================================================
ALU-12>config>log#
```

The *record-name* must be specified before configuring an accounting policy as **default**.

To configure an accounting policy for access ports, select a service record (for example, service-ingress-octets). To change the service record to another service record, re-enter the **record** command with the new *record-name* to replace the old *record-name*.

When configuring an accounting policy for network ports, select a network record. To change the network record to another network record, re-enter the **record** command with the new *record-name* to replace the old *record-name*.

Only one record may be configured in a single accounting policy. If changing the record switches it from network to service, or from service to network, the old *record-name* must be removed using the **no** form of this command. For example, to change an accounting policy configuration from a **network-egress-octets** record to a **service-ingress-octets** record, use the **no record** command and then enter the **service-ingress-octets** record.

Note: Collecting excessive statistics may adversely affect CPU usage and take up large amounts of storage space.

The **no** form of the command removes the record from the policy.

Default

n/a

Parameters

record-name

the accounting record name

to

Syntax

to file *log-file-id*

to no-file

Context

config>log>accounting-policy

Description

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

Default

No destination is specified

Parameters

log-file-id

the log file ID specifies the destination for the accounting records associated with this accounting policy. The characteristics of the log file ID, such as rollover and retention intervals, must have already been defined in the **config>log>file-id** context. A log file ID can only be used once.

The file is generated when the log file ID is first referenced. This command identifies the type of accounting file to be created. 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

5.12.2.1.3 Event control commands

event-control

Syntax

event-control *application-id* [*event-name* | *event-number*] **generate** [*severity-level*] [**throttle**] [**specific-throttle-rate** *events-limit* **interval** *seconds* |**disable-specific-throttle**]

event-control *application-id* [*event-name* | *event-number*] **suppress**

no event-control *application-id* [*event-name* | *event-number*]

Context

config>log

Description

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

Events are generated by an application and contain an event number and a 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. For example, to change event reporting for an external alarm output on the chassis, do the following:

1. Specify the application by using the **config>log>event-control>chassis** command.
2. Specify the event name or number by using the **config>log>event-control>chassis> extAlarmInput1Detected**command.
3. Specify whether the event is generated or suppressed by using the **config>log>event-control>chassis> extAlarmInput1Detected>generate** command.
4. Change the severity level (for example, major severity) by using the **config>log>event-control>chassis> extAlarmInput1Detected>generate>major** command.

Note: To display a list of events, use the **show>log>event-control** command.

Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are not generated. However, the generation of too many events may cause excessive overhead.

The **throttle** parameter enables event throttling for these events. The throttling rate is set globally for all events with the throttle-rate command. The throttling rate can also be configured independently for each log event by using the **specific-throttle-rate** parameter; this rate overrides the globally configured throttle rate for the specified log event.

The **no** form of the command resets the parameters to the default setting for events for the application or a specific event within the application. The *severity-level*, **generate**, and **suppress** options will also be reset to the initial values.

Default

Each event has a default suppress or generate state. To display a list of all events and the current configuration use the **event-control** command.

Parameters

application-id

the application whose events are affected by this event control filter

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

aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim, pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

Default none; this parameter must be explicitly specified

event-name | *event-number*

to generate, suppress, or revert to default for a single event, enter the specific number or event short name. If no event number or name is specified, the command applies to all events in the application. To display a list of all event short names use the **show>log>event-control** command.

Values *event name*: 32 characters maximum

event number: 0 to 4294967295

Default n/a

generate

specifies that a log event is created when this event occurs. The **generate** keyword can be used with two optional parameters: *severity-level* and **throttle**.

Default generate

severity-level

An ASCII string representing the severity level to associate with the specified generated events

Values one of: cleared, indeterminate, critical, major, minor, warning

Default the system-assigned severity level

throttle

specifies whether events of this type will be throttled

Default By default, event throttling is off for each specific event type. It must be explicitly enabled for each event type where throttling is needed. This makes backwards compatibility easier to manage.

suppress

indicates that the specified events will not be logged. If the **suppress** keyword is not specified, then the events are generated by default.

Default generate

specific-throttle-rate *events-limit*

configures an independent log event throttling rate for each log event, which overrides the globally configured throttle rate for the specified log event

Values 1 to 20000

seconds

the number of seconds that the specific throttling interval lasts

Values 1 to 1200

disable-specific-throttle

specifies to disable the **specific-throttle-rate**

throttle-rate

Syntax

throttle-rate *events* [**interval***seconds*]

no throttle-rate

Context

config>log

Description

This command configures an event throttling rate.

Parameters

events

specifies the number of log events that can be logged within the specified interval for a specific event. When the limit has been reached, any additional events of that type will be dropped, and 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 1 to 20000

Default 2000

seconds

specifies the number of seconds that an event throttling interval lasts

Values 1 to 1200

Default 1

5.12.2.1.4 Event handling commands

event-handling

Syntax

event-handling

Context

config>log

Description

This command enables the context to configure event handling in the Event Handler System (EHS).

handler

Syntax

[**no**] **handler** *event-handler-name*

Context

config>log>event-handling

Description

This command configures an event handler.

The **no** form of the command removes the specified event handler.

Parameters

event-handler-name

the name of the event handler, up to 32 characters in length

action-list

Syntax

action-list

Context

config>log>event-handling>handler

Description

This command enables the context to configure the event handler action list.

entry

Syntax

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

Context

config>log>event-handling>handler>action-list

Description

This command configures an event handler action-list entry. An action list consists of one or more entries. Each entry in the list references a configured script policy, which in turn references a configured script.

Multiple entries can be configured in the action list if multiple actions are required when an event triggers the event handler; for example, an event trigger results in the execution of different scripts. When the handler is triggered, it runs through the entries in sequence.

The **no** form of the command removes the specified action-list entry.

Parameters

entry-id

the identifier of the event handler action-list entry

Values 1 to 1500

min-delay

Syntax

min-delay [*delay*]

no min-delay

Context

config>log>event-handling>handler>action-list>entry

Description

This command specifies the minimum delay between subsequent executions of the action specified in this entry. This is useful, for example, to ensure that a script does not get triggered to execute too often.

Default

no min-delay

Parameters

delay

the delay time, in seconds

Values 1 to 604800

script-policy

Syntax

script-policy *policy-name* [**owner** *policy-owner*]

no script-policy

Context

config>log>event-handling>handler>action-list>entry

Description

This command specifies the script policy to use for this event handler action-list entry. The associated script is launched when the handler is triggered.

The script policy must already have been configured under the **config>system>script-control** context.

Default

no script-policy

Parameters

policy-name

the script policy name

policy-owner

the script policy owner associated with the script policy name

5.12.2.1.5 Event trigger commands

event-trigger

Syntax

event-trigger

Context

config>log

Description

This command enables the context to configure log events as triggers for event handlers in the EHS.

event

Syntax

[**no**] **event** *application-id event-name-id*

Context

config>log>event-trigger

Description

This command defines a specific log event that triggers the associated event handler. Further matching criteria can be applied (with the log-filter command) to only trigger certain handlers with certain instances of the log event.

The log event consists of an application ID and event ID.

The **no** form of the command removes the specified log event.

Parameters

application-id

the type of application that triggers the event

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim, pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

event-name-id

the numerical identifier or name of the event

Values 0 to 4294967295 | *event-name*: 32 characters maximum

trigger-entry

Syntax

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

Context

config>log>event-trigger>event

Description

This command configures a trigger entry for the specified log event. A trigger entry references a previously configured event handler. One or more trigger entries can be configured for the event.

Trigger entries can also be configured with a previously configured log filter.

The **no** form of the command removes the specified trigger entry.

Parameters

entry-id

the identifier of the event trigger entry

Values 1 to 1500

debounce

Syntax

debounce *occurrences* [**within** *seconds*]

no debounce

Context

config>log>event-trigger>event>trigger-entry

Description

This command configures how many times the specified log event occurs before an action is triggered (for example, an EHS script). The number of occurrences of the event can be optionally bounded by a time window. If no time window is specified, the action is triggered every specified Nth event.

Triggering occurs at the specified Nth event, not at the end of the time window.

Default

no debounce

Parameters

occurrences

the number of times the event must occur in order for EHS to trigger an action

Values 2 to 15

seconds

the time window, in seconds, in which the specified number of occurrences must happen in order for EHS to trigger an action

Values 1 to 604800

event-handler

Syntax

event-handler *event-handler*

no event-handler

Context

config>log>event-trigger>event>trigger-entry

Description

This command specifies the event handler to be used for this trigger entry. The event handler must have already been configured under the **config>log>event-handling>handler** context.

If the log event occurs and matches the criteria configured in the log filter (see log-filter), the event handler is triggered. When the event handler is triggered, the script that is referenced by the script policy that is in turn referenced by the event handler, is executed.

Parameters

event-handler

the name of the event handler

log-filter

Syntax

log-filter *filter-id*

no log-filter

Context

config>log>event-trigger>event>trigger-entry

Description

This command specifies the log filter to be used for this trigger entry. The log filter must have already been configured under the **config>log>filter** context.

The log filter defines the matching criteria that must be met in order for the log event to trigger the event handler. The log filter is applied to the log event, and if the filtering decision results in a **forward** action, the event handler is triggered.

Parameters

filter-id

the log filter identifier

Values 1 to 1500

5.12.2.1.6 Log file commands

encryption-key

Syntax

encryption-key *key* [**hash** | **hash2**]

no encryption-key

Context

config>log

Description

This command specifies the encryption key used by AES-265-CTR for log file encryption. The encryption key is used for all local log files on the system.

The **no** form of this command deletes the encryption key.

Parameters

key

specifies the encryption key

If the **hash** or **hash2** parameter is not configured, the key is entered in plaintext and the key length must be between 8 and 32 characters. A plaintext key cannot contain embedded nulls or end with "hash" or "hash2".

If the **hash** or **hash2** parameter is configured, the key is hashed and the key length must be between 1 and 64 characters.

hash

specifies that the key is entered and stored on the node in encrypted form

hash2

specifies that the key is entered and stored on the node in a more complex encrypted form. The **hash2** encryption scheme is node-specific and the key cannot be transferred between nodes.

file-id

Syntax

[**no**] **file-id** *log-file-id*

Context

config>log

Description

This command enables the context to configure a file ID template that is used as a destination for an event log or an accounting (billing) file.

The template defines the file location and characteristics of the destination for a log event message stream or for accounting and billing information. The *log-file-id* variable defined in this context is subsequently specified in the **to** command under **config>log>log-id** or **config>log>accounting-policy** contexts, to direct specific logging or accounting 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 accounting file that will be stored in the file system.

A file is created when the file ID defined by 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 filenames for a log or accounting file are created by the system (see the following table).

Table 41: Log filenames

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*
- *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 contains:

- 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 (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), the log file will not become operational even if the compact flash card is replaced. Enter a **clear log** command or a **shutdown**/**no shutdown** command sequence to reinitialize the file.

If the location fails (for example, the compact flash card fills up during the write process), a trap is sent.

The **no** form of the command removes the file ID from the configuration. A file ID can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

Default

n/a

Parameters

log-file-id

the file identification number for the file, expressed as a decimal integer

Values 1 to 99

location

Syntax

location *cflash-id*

no location

Context

config>log>file-id

Description

This command specifies the location where the log or accounting billing file will be created.

The **location** command is optional. If the **location** command is not explicitly configured, log and accounting files will be created on cf3: for the following:

- 7705 SAR-8 Shelf V2
- 7705 SAR-A
- 7705 SAR-Ax
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-M
- 7705 SAR-Wx
- 7705 SAR-X

For the 7705 SAR-18, log files are created by default on cf1: and accounting files are created by default on cf2:. There are no overflows onto other devices.

Note: The 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-Wx, 7705 SAR-Hc, and 7705 SAR-X do not have field-replaceable compact flash drives; they are shipped with integrated flash memory that is used to store system boot software, OS software, and configuration files and logs. The flash memory is identified as cf3-A: by the system. On the 7705 SAR-X and 7705 SAR-Ax, the flash memory is 512 Mbytes; for the other platforms, the flash memory is 256 Mbytes.

When multiple **location** commands are entered in a single file ID context, the last command overwrites the previous command.

When the location of a file ID that is associated with an active log ID is changed, the log events are not immediately written to the new location. The new location does not take effect until the log rolls over, either because the rollover period has expired or a **clear>log** *log-id* command is entered to manually roll over the log file.

When creating log or accounting files, the designated location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available, an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A medium severity trap is issued to indicate that the compact flash is either not available or that no space is available on the specified flash.

A high-priority alarm condition is raised if the compact flash device for this file ID is not present or if there is insufficient space available. If space does becomes available, the alarm condition will be cleared.

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

Default

For the 7705 SAR-8 Shelf V2, 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-M, 7705 SAR-Wx, and 7705 SAR-X, log and accounting files are created on cf3:

For the 7705 SAR-18, log files are created on cf1: and accounting files are created on cf2:

Parameters

cflash-id

specifies the location of the flash

Values *cflash-id*: cf3: for all platforms; also cf1: or cf2: for the 7705 SAR-18

rollover

Syntax

rollover *minutes* [**retention** *hours*]

no rollover

Context

config>log>file-id

Description

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

An event or accounting log is actually composed of multiple individual files. The system creates a new file for the log based on the rollover time, expressed in minutes.

The **retention** option, expressed in hours, allows you to modify the default time that the file is kept in the system. The retention time is based on the rollover time of the file. The retention time is used as a factor to determine which files should be deleted first as the file space becomes full.

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

Default

rollover 1440

retention 12

Parameters

minutes

the rollover time, in minutes

Values 5 to 10080

hours

the retention period, in hours, expressed as a decimal integer. The retention period is based on the creation time of the file. The file becomes a candidate for removal when the creation timestamp + rollover time + retention time is less than the current timestamp.

Values 1 to 500

5.12.2.1.7 Log filter commands

filter

Syntax

[**no**] **filter** *filter-id*

Context

config>log

Description

This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.

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

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

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

Default

No event filters are defined.

Parameters

filter-id

uniquely identifies the filter

Values 1 to 1001

Default 1001

default-action

Syntax

default-action {**drop** | **forward**}

no default-action

Context

config>log>filter

Description

The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.

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

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

Default

default-action forward

Parameters

drop

the events that are not explicitly forwarded by an event filter match are dropped

forward

the events that are not explicitly dropped by an event filter match are forwarded

entry

Syntax

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

Context

config>log>filter

Description

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

Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

An entry may have no match criteria defined (in which case, everything matches) but must have at least the **action** keyword for it to be considered complete. Entries without the **action** keyword will be considered incomplete and rendered inactive.

The **no** form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log IDs where the filter is applied.

Default

No event filter entries are defined. An entry must be explicitly configured.

Parameters

entry-id

uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 to 999

action

Syntax

action {**drop** | **forward**}

no action

Context

config>log>filter>entry

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 commands are entered, the last command will overwrite the previous command.

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

Default

no action

Parameters

drop

specifies that packets matching the entry criteria will be dropped

forward

specifies that packets matching the entry criteria will be forwarded

match

Syntax

[**no**] **match**

Context

config>log>filter>entry

Description

This command enables the context to enter 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, then all the criteria must be satisfied and functional before the action associated with the match is executed.

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

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

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

Default

No match context is defined.

application

Syntax

application {**eq** | **neq**} *application-id*

no application

Context

config>log>filter>entry>match

Description

This command adds a TiMOS application as an event filter match criterion.

A TiMOS application is the software entity that reports the event. Examples of applications include: IP, MPLS, CLI, and SERVICES. Only one application can be specified per entry.

When multiple **application** commands are entered, the last command will overwrite the previous command.

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

Default

no application

Parameters

eq

specifies that the matching criteria should be equal to the specified value

neq

specifies that the matching criteria should not be equal to the specified value

application-id

the application name string

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim, pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

message

Syntax

message {**eq** | **neq**}**pattern** *pattern* [**regexp**]

no message

Context

config>log>filter>entry>match

Description

This command adds system messages as a match criterion.

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

Parameters

eq

specifies that the matching criteria should be equal to the specified value

neq

specifies that the matching criteria should not be equal to the specified value

pattern

specifies a message up to 400 characters in length to be used in the match criteria

regexp

specifies the type of string comparison to use to determine if the log event matches the value of **message** command parameters. When the **regexp** keyword is specified, the string in the **message** command is a regular expression string that will be matched against the message string in the log event being filtered. When the **regexp** keyword is not specified, the default matching algorithm used is a basic substring match.

number

Syntax

number {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *event-id*

no number

Context

config>log>filter>entry>match

Description

This command adds a TiMOS application event number as a match criterion.

TiMOS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. If multiple **number** commands are entered, the last command overwrites the previous command.

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

Default

no event-number

Parameters

eq | neq | lt | lte | gt | gte

this operator specifies the type of match. Valid operators are listed in the following table.

Table 42: Valid match operators for event numbers

Operator	Notes
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

event-id

the event ID, expressed as a decimal integer

Values 1 to 4294967295

router

Syntax

router {**eq** | **neq**} *router-instance* [**regexp**]

no router

Context

config>log>filter>entry>match

Description

This command specifies the log event matches for the router.

Parameters

eq

specifies that the matching criteria should be equal to the specified value

neq

specifies that the matching criteria should not be equal to the specified value

router-instance

specifies a router name up to 32 characters to be used in the match criteria

regexp

specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** keyword is specified, the string in the **router** command is a regular expression string that will be matched against the router string in the log event being filtered. When the **regexp** keyword is not specified, the **router** command string is matched exactly by the event filter.

severity

Syntax

severity {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *severity-level*

no severity

Context

config>log>filter>entry>match

Description

This command adds an event severity level as a match criterion. Only one **severity** command can be entered per event filter entry. When multiple **severity** commands are entered, the last command overwrites the previous command.

The **no** form of the command removes the severity match criterion.

Default

no severity

Parameters

eq | neq | lt | lte | gt | gte

this operator specifies the type of match. Valid operators are listed in the following table.

Table 43: Valid operators for event severity

Operator	Notes
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

severity-level

the ITU severity level number. The following table lists severity levels and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Table 44: Severity levels

Severity number	Severity level
1	Cleared
2	Indeterminate (info)
3	Critical
4	Major
5	Minor
6	Warning

subject

Syntax

subject {**eq** | **neq**} *subject* [**regexp**]

no subject

Context

config>log>filter>entry>match

Description

This command adds an event subject as a match criterion.

The *subject* is the entity for which the event is reported, such as a port. In this case, the *port-id* string would be the *subject*.

Only one **subject** command can be entered per event filter entry. If multiple **subject** commands are entered, the last command overwrites the previous command.

The **no** form of the command removes the subject match criterion.

Default

no subject

Parameters

eq

specifies that the matching criteria should be equal to the specified value

neq

specifies that the matching criteria should not be equal to the specified value

subject

a string used as the subject match criterion

regexp

specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered.

When the **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

5.12.2.1.8 Syslog commands

syslog

Syntax

[**no**] **syslog** *syslog-id*

Context

config>log

Description

This command enables the context to configure a syslog target host that is capable of receiving selected syslog messages from the 7705 SAR.

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.

Default

No syslog IDs are defined.

Parameters

syslog-id

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

Description

This command associates the syslog target host IP address with the syslog ID.

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

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

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

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

Default

no address

Parameters

ip-address

the IP address of the syslog target host

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:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

facility

Syntax

facility *syslog-facility*

no facility

Context

config>log>syslog

Description

This command configures the facility code for messages sent to the syslog target host.

Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last facility code entered overwrites the previous facility code.

If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.

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

Default

local7

Parameters

syslog-facility

the syslog facility name for the event type being sent to the syslog target host. Valid codes are as per RFC 3164, *The BSD syslog Protocol.*

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

level

Syntax

level *syslog-level*

no level

Context

config>log>syslog

Description

This command configures the syslog message severity level threshold. All messages with a severity level equal to or higher than the threshold are sent to the syslog target host.

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

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

Default

info

Parameters

syslog-level

the threshold severity level value, as described in the following table. See Table 35: Event severity levels for the numeric values associated with the severity levels.

Table 45: Threshold severity level values

Configured severity	Definition
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical condition
Error	Error condition
Warning	Warning condition
Notice	Normal but significant condition
Info	Informational messages
Debug	Debug-level messages

Values emergency, alert, critical, error, warning, notice, info, or debug

log-prefix

Syntax

log-prefix *log-prefix-string*

no log-prefix

Context

config>log>syslog

Description

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

RFC 3164, *The BSD syslog Protocol,* allows an alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.

Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.

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

Default

no log-prefix

Parameters

log-prefix-string

an alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

port

Syntax

port *value*

no port

Context

config>log>syslog

Description

This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

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

Default

no port

Parameters

value

the configured UDP port number used when sending syslog messages

Values 0 to 65535

5.12.2.1.9 Logging destination commands

log-id

Syntax

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

Context

config>log

Description

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

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

A maximum of 100 logs can be configured.

Before an event can be associated with this *log-id*, the **log-id>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.

The **no** form of the command deletes the log destination ID from the configuration.

Default

No log destinations are defined

Parameters

log-id

the log ID number, expressed as a decimal integer

Values 1 to 100

filter

Syntax

filter *filter-id*

no filter

Context

config>log>log-id

Description

This command associates an event filter policy with the log destination.

The **filter** command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the *log-id*. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination **snmp-trap-group**.

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

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

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

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

Default

no filter

Parameters

filter-id

the event filter policy ID that is used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in the **config>log>filter** *filter-id* context. Log ID 100 is preconfigured by the system as a Severe Event Log that is associated with filter policy 1001 by default.

Values 1 to 1001

from

Syntax

from {[**main**] [**security**] [**change**] [**debug-trace**]}

no from

Context

config>log>log-id

Description

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

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

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

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

Default

no from

Parameters

main

instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that

are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the filter (log destination) command.

security

instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access, or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the filter (log destination) command.

change

instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the filter (log destination) command.

debug-trace

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

to console

Syntax

to console

Context

config>log>log-id

Description

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 command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

to file

Syntax

to file *log-file-id*

Context

config>log>log-id

Description

This command instructs the events selected for the log ID to be directed to a specified file.

The command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

Parameters

log-file-id

instructs the events selected for the log ID to be directed to the *log-file-id*. The characteristics of the *log-file-id* referenced here must have already been defined in the **config>log>file-id** *log-file-id* context.

Values 1 to 99

to memory

Syntax

to memory [*size*]

Context

config>log>log-id

Description

This command instructs the events selected for the log ID to be directed to a memory file. A memory file is a circular buffer. When the file is full, each new entry replaces the oldest entry in the log.

The command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

Parameters

size

indicates the number of events that can be stored in the memory log

Values 50 to 3000

Default 100

to session

Syntax

to session

Context

config>log>log-id

Description

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 **to session** configuration is removed. A log ID with a session destination is saved in the configuration file but the **to session** part of the configuration is not stored.

The command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

to snmp

Syntax

to snmp [*size*]

Context

config>log>log-id

Description

This command instructs the alarms and traps to be directed to the **snmp-trap-group** associated with the *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 command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

Parameters

size

defines the number of events stored in this memory log

Values 50 to 3000

Default 100

to syslog

Syntax

to syslog *syslog-id*

Context

config>log>log-id

Description

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 1 kbyte.

The command is one of the **to** commands used to specify the log ID destination. A **to** command is mandatory when configuring a log destination.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command can only be set once. It cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed and then recreated.

Default

No destination is specified

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

Description

This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default

utc

Parameters

local

specifies that timestamps are written in the system's local time

utc

specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

5.12.2.1.10 SNMP trap group commands

snmp-trap-group

Syntax

[**no**] **snmp-trap-group** *log-id*

Context

config>log

Description

This command enables the context to configure a group of SNMP trap receivers and their operational parameters for a specified *log-id*.

A trap 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 in order for SNMP traps to be sent.

To suppress the generation of all alarms and traps, see the event-control command. To suppress alarms and traps that are sent to this *log-id*, see the filter (log destination) 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 the command deletes the SNMP trap group.

Default

There are no default SNMP trap groups.

Parameters

log-id

the log ID value of a log configured in the to snmp context. Alarms and traps cannot be sent to the trap receivers until a valid *log-id* exists.

Values 1 to 99

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**}]

no trap-target*name*

Context

config>log>snmp-trap-group

Description

This command adds or modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a 7705 SAR, such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the to console, 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 IP address of the trap receiver
- the UDP port used to send the SNMP trap
- SNMP version
- SNMP community name for SNMPv1 and SNMPv2c receivers
- security name and level for SNMPv3 trap receivers

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

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

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

Note: 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 7705 SAR event log when multiple event logs are directed to the same IP address and port destination.

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

Default

No SNMP trap targets are defined.

Parameters

name

specifies the name of the trap target, up to 28 characters in length

ip-address

the IP address of the trap receiver. Only one IP address destination can be specified per trap destination group.

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 to FFFF]H

d: [0 to 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.

Values 0 to 65535

Default 162

snmpv1 | snmpv2c | snmpv3

specifies the SNMP version format to use for traps sent to the trap receiver

Values

snmpv1	Selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** parameter 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 instead of the *snmpv3securityName* that is used by **snmpv3**.
snmpv2c	Selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** parameter 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 instead of the *security-name* that is used by **snmpv3**.
snmpv3	Selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** parameter 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* instead of the community string used by **snmpv1** or **snmpv2c**.

Default snmpv3

notify-community *communityName* **|** *snmpv3SecurityName*

specifies the community string for **snmpv1** or **snmpv2c**, or the **snmpv3** *security-name*. If no **notify-community** parameter is configured, then no alarms or traps are issued for the trap destination. If the SNMP version is modified, the **notify-community** parameter must be changed to the correct form for the SNMP version.

Values

communityName	the community string as required by the **snmpv1** or **snmpv2c** trap receiver. The community string can be an ASCII string up to 32 characters in length.
snmpv3SecurityName	the security name as defined in the **config>system>security>user** context for SNMP

v3. The *snmpv3SecurityName* can be an ASCII string up to 32 characters in length.

security-level {no-auth-no-privacy | auth-no-privacy | privacy}

specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

Values

no-auth-no-privacy	Specifies that no authentication and no privacy (encryption) are required
auth-no-privacy	Specifies that authentication is required but no privacy (encryption) is required. When this option is configured, the *security-name* must be configured for authentication.
privacy	Specifies that both authentication and privacy (encryption) are required. When this option is configured, the *security-name* must be configured for authentication and privacy.

Default No default. The security level must be specified when configuring an SNMPv3 trap receiver.

5.12.2.2 Show commands

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

accounting-policy

Syntax

accounting-policy [*acct-policy-id*] [**access** | **network**] [**associations**]

Context

show>log

Description

This command displays accounting policy information.

Parameters

acct-policy-id

the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer

Values 1 to 99

access

only displays access accounting policies

network

only displays network accounting policies

associations

only displays accounting policy associations

Output

The following output is an example of accounting policy information, and Table 46: Accounting policy field descriptions describes the fields.

Output example

```
A:ALU-1# show log accounting-policy
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
1      access  No  Up    Up    15        1    service-ingress-packets
2      access  Yes Up    Up    15        2    service-ingress-octets
===============================================================================
A:ALU-1#
```

```
A:ALU-1# show log accounting-policy 10
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3    service-ingress-packets

Description      : (Not Specified)
Data Loss Count  : 0               Data Loss TimeStamp: N/A

This policy is applied to:
    Svc Id: 100  SAP : 1/1/8:0     Collect-Stats
    Svc Id: 101  SAP : 1/1/8:1     Collect-Stats
    Svc Id: 102  SAP : 1/1/8:2     Collect-Stats
    Svc Id: 106  SAP : 1/1/8:6     Collect-Stats
    Svc Id: 107  SAP : 1/1/8:7     Collect-Stats
    Svc Id: 108  SAP : 1/1/8:8     Collect-Stats
    Svc Id: 109  SAP : 1/1/8:9     Collect-Stats
...
===============================================================================
A:ALU-1#
```

```
A:ALU-1# show log accounting-policy access
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3    service-ingress-packets
```

```
===============================================================================
A:ALU-1#
```

Table 46: Accounting policy field descriptions

Label	Description
Policy ID	The identifying value assigned to a specific policy
Type	Identifies the accounting policy 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
	none: indicates no accounting policy types assigned
Def	Yes: indicates that the policy is a default policy
	No: indicates that the policy is not a default policy
Admin State	Displays the administrative state of the policy
	Up: indicates that the policy is administratively enabled
	Down: indicates that the policy is administratively disabled
Oper State	Displays the operational state of the policy
	Up: indicates that the policy is operationally up
	Down: indicates that the policy is operationally down
Intvl	Displays the interval, in minutes, in which statistics are collected and written to their destination. The default depends on the record name type.
File ID	The log destination
Record Name	The accounting record name that represents the configured record type
Description	The description of the accounting policy
Data Loss Count	The number of times a statistics data loss has occurred
Data Loss Timestamp	The timestamp of the last data loss occurrence. If there are no losses, the timestamp is N/A.
This policy is applied to	Specifies the entities that the accounting policy is applied to

accounting-records

Syntax

accounting-records

Context

show>log

Description

This command displays accounting policy record names.

Output

The following output is an example of accounting policy record information, and Table 47: Accounting records field descriptions describes the fields.

Output example

```
A: ALU-1# 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
11       combined-network-ing-egr-octets   15
12       combined-service-ing-egr-octets   5
13       complete-service-ingress-egress   5
32       saa                               5
54       complete-network-ing-egr          15
===========================================================
A:ALU-1#
```

Table 47: Accounting records field descriptions

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

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 an application list (not all applications apply to the 7705 SAR).

Output example

```
A:ALU-1# show log applications
================================
Log Event Application Names
================================
Application Name
--------------------------------
APS
ATM
BFD
BGP
CHASSIS
CPMHWFILTER
DEBUG
DHCP
DHCPS
DOT1X
EFM_OAM
ERING
ETH_CFM
FILTER
FIREWALL
FR
IGMP
IGMP_SNOOPING
IP
IPSEC
IPSEC_CPM
ISIS
LAG
LDP
LLDP
LOGGER
MCPATH
MC_REDUNDANCY
MIRROR
MLD
MLD_SNOOPING
MPLS
MWMGR
```

```
NGE
NTP
OAM
OSPF
PIM
PIM_SNOOPING
PORT
PPP
PTP
QOS
RADIUS
RIP
RIP_NG
ROUTE_NEXT_HOP
ROUTE_POLICY
RSVP
SCADA
SECURITY
SNMP
STP
SUB_HOST_TRK
SVCMGR
SYSTEM
TIP
TSS
USER
VRRP
VRTR
================================
A:ALU-1#
```

event-control

Syntax

event-control [*application-id* [*event-name* | *event-number*]]

event-control *application-id event-name***detail**

Context

show>log

Description

This command displays event control settings for events, including whether the event is suppressed or generated, and the severity level for the event.

If no options are specified, all events, alarms, and traps are listed.

Parameters

application-id

displays event control for the specified application

Values aps, atm, cflowd, bgp, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim,

pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

Default all applications

event-name

displays event control for the named application event

Values 32 characters maximum

Default all events for the application

event-number

displays event control for the specified application event number

Values 0 to 4294967295

Default all events for the application

detail

displays detailed event-control information

Output

The following output is an example of event control information, and Table 48: Event control field descriptions describes the fields. Because the output is very large, only a sample of the events are shown here.

Output example

```
A:gal171# show log event-control
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
ATM:
   2004 tAtmTcSubLayerDown               MI  gen          0           0
   2005 tAtmTcSubLayerClear              MI  gen          0           0
L  2006 atmVclStatusChange               WA  gen          0           0
...
CHASSIS:
   2001 cardFailure                      MA  gen          4           0
   2002 cardInserted                     MI  gen          3           0
   2003 cardRemoved                      MI  gen          8           0
   2004 cardWrong                        MI  gen          0           0
   2005 EnvTemperatureTooHigh            MA  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          0           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          0          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 extAlarmInput1Detected           CR  gen          0          0
   2058 extAlarmInput2Detected           MA  gen          0          0
   2059 extAlarmInput3Detected           MA  gen          0          0
   2060 extAlarmInput4Detected           MI  gen          0          0
   2061 extAlarmCleared                  MA  gen          0          0
   2062 syncIfTimingExternAlarm          MI  gen          0          0
   2063 syncIfTimingExternAlarmClear     MI  gen          0          0
   2064 cardBgDiagsFault                 MI  gen          0          0
   2065 fanCriticalFailure               CR  gen          0          0
   2066 fanMinorFailure                  MI  gen          0          0
   2067 cardSyncFileNotPresent           MI  gen          0          0
   2058 tmnxEqMdaXplError                MI  sup          0          0
...
DEBUG:
L  2001 traceEvent                       MI  gen          0          0
DOT1AG:
   2001 dot1agCfmFaultAlarm              MI  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
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
....

....
USER:
L  2001 cli_user_login                   MI  gen          2          0
L  2002 cli_user_logout                  MI  gen          1          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          48
L  2010 snmp_user_set                    MI  sup          0           0
L  2011 cli_config_io                    MI  gen       4357           0
===============================================================================
A:ALU-1#
```

Table 48: Event control field descriptions

Label	Description
Application	The application name
ID#	The event ID number within the application L ID#: an "L" in front of an ID represents event types that do not generate an associated SNMP notification. Most events generate a notification; only the exceptions are marked with a preceding "L".
Event Name	The event name
P	CL: the event has a cleared severity/priority
	CR: the event has critical severity/priority
	IN: the event has indeterminate severity/priority
	MA: the event has major severity/priority
	MI: the event has minor severity/priority
	WA: the event has warning severity/priority
g/s	gen: the event is generated/logged by event control
	sup: the event is suppressed/dropped by event control
	thr: specifies that throttling is enabled
Logged	The number of events logged/generated
Dropped	The number of events dropped/suppressed

event-handling

Syntax

event-handling

Context

show>log

Description

This command enables the context to display Event Handling System (EHS) information.

handler

Syntax

handler [*handler-name*]

handler detail

Context

show>log>event-handling

Description

This command displays event handler information.

Parameters

handler-name

specifies an event handler name

detail

displays detailed information for all event handlers

Output

The following is an example of event handler information, and Table 49: Event handler field descriptions describes the fields.

Output example

```
A:7705:Dut-C# show log event-handling handler "handler_1"
===============================================================================
Event Handling System - Handlers
===============================================================================
===============================================================================
Handler          : handler_1
===============================================================================
Description      : test_handler
Admin State      : up                                Oper State : up

-------------------------------------------------------------------------------
Handler Execution Statistics
  Success        : 1
  Err No Entry   : 0
  Err Adm Status : 0
Total            : 1

-------------------------------------------------------------------------------
Handler Action-List Entry
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Entry-id         : 1
Description      : test_entry
Admin State      : up                                Oper State : up
```

```
Script
  Policy Name    : script_policy_1
  Policy Owner   : TiMOS CLI
Min Delay        : 0
Last Exec        : 05/24/2018 19:03:31
-------------------------------------------------------------------------------
Handler Action-List Entry Execution Statistics
  Success        : 1
  Err Mn Delay   : 0
  Err Launch     : 0
  Err Adm Status : 0
Total            : 1
===============================================================================
```

Table 49: Event handler field descriptions

Label	Description
Handler	The name of the event handler
Description	The event handler description string
Admin State	The administrative state of the event handler
Oper State	The operational state of the event handler
Handler Execution Statistics	
Success	The number of times that the event handler was successfully triggered
Err No Entry	The number of times that the event handler failed to trigger due to no action-list entry
Err Adm Status	The number of times that the event handler was not executed because the entry was administratively disabled
Total	The total number of times that the event handler attempted execution
Handler Action-List Entry	
Entry-id	The action-list entry identifier
Description	The action-list entry description string
Admin State	The administrative state of the action-list entry
Oper State	The operational state of the action-list entry
Script	
Policy Name	The name of the related script policy
Policy Owner	The owner of the related script policy

Label	Description
Min Delay	The configured minimum delay time between subsequent executions of the action specified in the entry
Last Exec	The timestamp of the last successful execution of the action-list entry
Handler Action-List Entry Execution Statistics	
Success	The number of times that the action-list entry was successfully queued to run. For a script-policy entry, this indicates that the script request has been enqueued but does not necessarily indicate that the script has successfully launched or completed.
Err Mn Delay	The number of times that the action-list entry attempted to execute before the minimum delay time expired
Err Launch	The number of times that the action-list entry was not successfully queued to run. This could be caused by a number of conditions, including a full script request input queue.
Err Adm Status	The number of times that the action-list entry was not executed because the entry was administratively disabled
Total	The total number of times that the action-list entry attempted execution

information

Syntax

information

Context

show>log>event-handling

Description

This command displays general information about EHS, as well as handler and trigger statistics.

Output

The following is an example of EHS information.

Output example

```
A:7705:Dut-C# show log event-handling information
===============================================================================
Event Handling System - Event Trigger Statistics
===============================================================================

-------------------------------------------------------------------------------
Application Name
```

```
Event Id                    Total     Success   ErrNoEntry AdmStatus
-------------------------------------------------------------------------------
OAM
2001                        0         0         0          0
  -----------------------------------------------------------------------------
   Entry FilMatch  Trigger   Debounce  FilFail   ErrAdmSta  ErrFilter ErrHandler
  -----------------------------------------------------------------------------
   1     0         0         0         0         0          0         0
   10    0         0         0         0         0          0         0
  -----------------------------------------------------------------------------
   SUM   0         0         0         0         0          0         0
_______________________________________________________________________________
Application Name
Event Id                    Total     Success   ErrNoEntry AdmStatus
-------------------------------------------------------------------------------
OAM
2004                        0         0         0          0
  -----------------------------------------------------------------------------
   Entry FilMatch  Trigger   Debounce  FilFail   ErrAdmSta  ErrFilter ErrHandler
  -----------------------------------------------------------------------------
   1     0         0         0         0         0          0         0
  -----------------------------------------------------------------------------
   SUM   0         0         0         0         0          0         0
===============================================================================
EVENTS PROCESSED            Total     Success   ErrNoEntry AdmStatus
-------------------------------------------------------------------------------
                            0         0         0          0
===============================================================================
===============================================================================
Event Handling System - Event Handler Statistics
===============================================================================
_______________________________________________________________________________
Handler                     Total     Success   ErrNoEntry AdmStatus
handler_1                   0         0         0          0
  -----------------------------------------------------------------------------
   Entry Id        Launch    MinDelay  ErrLaunch  ErrAdmSta
  -----------------------------------------------------------------------------
   1               0         0         0          0
  -----------------------------------------------------------------------------
   SUMMARY         0         0         0          0
===============================================================================
HANDLERS SUMMARY            Total     Success   ErrNoEntry AdmStatus
-------------------------------------------------------------------------------
                            0         0         0          0
===============================================================================
```

scripts

Syntax

scripts

Context

show>log>event-handling

Description

This command displays handler configuration and script run queue information.

Output

The following is an example of script information.

Output example

```
A:7705:Dut-C# show log event-handling scripts
===============================================================================
Event Handling System - Script Policy Association
===============================================================================
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
Event Handling System - Script Association
===============================================================================
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
Event Handling System - Script Launched List
===============================================================================
Run #     Script owner               Script name                 Script state
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================
```

event-parameters

Syntax

event-parameters [*application-id* [*event-name* | *event-number*]]

Context

show>log

Description

This command displays the common parameters and specific parameters of log event or of all log events. This display lets a user know what parameters can be passed from a triggering event to the triggered EHS script.

Parameters

application-id

displays event parameters for the specified application

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim, pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

Default all applications

event-name

displays event parameters for the named application event

Values 32 characters maximum

Default all events for the application

event-number

displays event parameters for the specified application event number

Values 0 to 4294967295

Default all events for the application

Output

The following is an example of log event parameter information.

Output example

```
# show log event-parameters "oam" 2001
===============================================================================
Common Event Parameters
        appid
        name
        eventid
        severity
        subject
        gentime
Event Specific Parameters
        tmnxOamPingCtlOwnerIndex
        tmnxOamPingCtlTestIndex
        tmnxOamPingCtlTgtAddrType
        tmnxOamPingCtlTgtAddress
        tmnxOamPingResultsTestRunIndex
        tmnxOamPingResultsOperStatus
        tmnxOamPingResultsMinRtt
        tmnxOamPingResultsMaxRtt
        tmnxOamPingResultsAverageRtt
        tmnxOamPingResultsRttSumOfSquares
        tmnxOamPingResultsRttOFSumSquares
        tmnxOamPingResultsMtuResponseSize
        tmnxOamPingResultsSvcPing
        tmnxOamPingResultsProbeResponses
        tmnxOamPingResultsSentProbes
        tmnxOamPingResultsLastGoodProbe
        tmnxOamPingCtlTestMode
        tmnxOamPingHistoryIndex
===============================================================================
```

file-id

Syntax

file-id [*log-file-id*]

Context

show>log

Description

This command displays event log file 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 for the event log file.

Parameters

log-file-id

displays detailed information for the specified event log file

Values 1 to 99

Output

The following output is an example of event log file information, and Table 50: Log file summary field descriptions describes the fields.

Output example

```
A:ALU-1# show log file-id
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                              location  location  location
---------------------------------------------------------------
1           60         4        cf3:      none      none
2           60         3        cf3:      none      none
3         1440        12        cf3:      none      none
10        1440        12        cf3:      none      none
11        1440        12        cf3:      none      none
15        1440        12        cf3:      none      none
20        1440        12        cf3:      none      none
===============================================================
A:ALU-1#
```

```
A:ALU-1# show log file-id 10
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                              location  location  location
---------------------------------------------------------------
10        1440        12      cf3:      none      none
Description : Main
===============================================================
===============================================================
File Id 10 Location cf3:
===============================================================
file name                                 expired   state
---------------------------------------------------------------
cf3:\log\log0302-20060501-012205        yes       complete
cf3:\log\log0302-20060501-014049        yes       complete
cf3:\log\log0302-20060501-015344        yes       complete
```

```
cf3:\log\log0302-20060501-015547        yes       in progress
===============================================================
```

Table 50: Log file summary field descriptions

Label	Description
file-id	The log file ID
rollover	The rollover time for the log file, which is the amount of time before the file is partitioned into a new file.
retention	The retention time for the file in the system, which is how long the file should be retained in the file system
admin location	The flash device specified for the file location
	none: indicates no specific flash device was specified
backup location	The backup compact flash device specified for the file location
oper location	The actual flash device on which the log file exists
file name	The complete pathname of the file associated with the log ID
expired	Indicates whether the retention period for this file has passed
state	in progress: indicates the current open log file
	complete: indicates the old log file

filter-id

Syntax

filter-id [*filter-id*]

Context

show>log

Description

This command displays event log filter policy information. If you specify a filter ID, the command also displays the filter match criteria.

Parameters

filter-id

displays detailed information for the specified event filter policy ID

Values 1 to 1001

Output

The following outputs are examples of event log filter policy information:

- filter ID summary information (Output example, Table 51: Filter ID summary field descriptions)
- filter ID information with match criteria specified (Output example, Table 52: Filter ID match criteria field descriptions)

Output example

```
*A:ALU-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:ALU-48>config>log#
```

Table 51: Filter ID summary field descriptions

Label	Description
Filter Id	The event log filter ID
Applied	no: the event log filter is not currently in use by a log ID
	yes: the event log filter is currently in use by a log ID
Default Action	drop: the default action for the event log filter is to drop events not matching filter entries
	forward: the default action for the event log filter is to forward events not matching filter entries
Description	The description string for the filter ID

Output example

```
*A:ALU-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
-------------------------------------------------------------------------------
===============================================================================
```

Table 52: Filter ID match criteria field descriptions

Label	Description
Entry-id	The event log filter entry ID
Action	default: there is no explicit action for the event log filter entry and the filter's default action is used on matching events
	drop: the action for the event log filter entry is to drop matching events
	forward: the action for the event log filter entry is to forward matching events
Description: (Entry-id)	The description string for the event log filter entry
Application	The event log filter entry application match criterion
Event Number	The event log filter event ID match criterion
Severity	cleared: the event log filter severity match is cleared
	indeterminate: the event log filter entry application event severity indeterminate match criterion
	critical: the event log filter entry application event severity critical match criterion
	major: the event log filter entry application event severity cleared match criterion
	minor: the event log filter entry application event severity minor match criterion
	warning: the event log filter entry application event severity warning match criterion
Subject	Displays the event log filter entry **subject** string match criterion
Router	Displays the event log filter entry **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

Label	Description
	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

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 statistics, and Table 53: Log collector field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-1#
```

Table 53: Log collector field descriptions

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 that defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Status	Enabled: logging is enabled
	Disabled: logging is disabled
Dest. Type:	Console: a log created with the console type destination displays events to the physical console device Events are displayed to the console screen whether a user is logged in to the console or not. A user logged in to the console device or connected to the CLI via a remote Telnet or SSH session can also create a log with a destination type of 'session'. Events are displayed to the session device until the user logs off. When the user logs off, the 'session' type log is deleted.
	Syslog: all selected log events are sent to the syslog address
	SNMP traps: events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables
	File: all selected log events are directed to a file on the CSM's compact flash disk
	Memory: all selected log events are 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

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 log file or memory log ID. The log ID must have a destination of an SNMP or log file or a memory log for this parameter to be used.

Values 1 to 100

Default displays the event log summary

severity-level

displays only events with the specified and higher severity

Values cleared, indeterminate, critical, major, minor, and warning

Default all severity levels

application

displays only events generated by the specified application

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, ering, eth_cfm, filter, firewall, igmp, igmp_snooping, ip, ipsec, isis, lag, lcr, ldp, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, mwmgr, ntp, oam, ospf, pcap, pim, pim_snooping, port, ppp, ptp, radius, rip, rip_ng, route_policy, rsvp, scada, security, snmp, stp, svcmgr, system, tss, user, vrrp, vrtr

Default all applications

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 are displayed unless the count parameter is present, in which case the number of entries displayed is limited by the count.

Values 1 to 4294967295

Default all sequence numbers

count

limits the number of log entries displayed to the number specified

Values 1 to 4294967295

Default all log entries

router-instance

specifies a router name up to 32 characters to be used in the display criteria

expression

specifies to use a regular expression as match criteria for the router instance string

subject

displays only log entries matching the specified text subject string. The subject is the object affected by the event; for example, the *port-id* would be the subject for a link-up or link-down event.

regexp

specifies to use a regular expression as parameters with the specified *subject* string

ascending | descending

specifies the log sort direction. Logs are normally shown from the newest entry to the oldest in descending sequence number order on the screen. When using the ascending parameter, the log will be shown from the oldest to the newest entry.

Default Descending

Output

The following output is an example of event log summary information, and Table 54: Log ID field descriptions describes the fields.

Output example

```
A:ALU-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:ALU-1#
```

Table 54: Log ID field descriptions

Label	Description
Log Id	An event log destination
Source	no: the event log filter is not currently in use by a log ID
	yes: the event log filter is currently in use by a log ID
	M: the event source for the log ID is the Main event category
	C: the event source for the log ID is the Change event category
	none: the event log filter is currently in use by a log ID
Filter ID	The value is the index to the entry that defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Admin State	Up: indicates that the administrative state is up
	Down: indicates that the administrative state is down
Oper State	Up: indicates that the operational state is up
	Down: indicates that the operational state is down
Logged	The number of events that have been sent to the log sources that were forwarded to the log destination
Dropped	The number of events that have been 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, then all entries are dropped.
	Syslog: all selected log events are sent to the syslog address
	SNMP traps: events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables
	File: all selected log events are directed to a file on the CSM's compact flash disk

Label	Description
	Memory: all selected log events are directed to an in-memory storage area
Dest ID	The event log stream destination
Size	The allocated memory size for the log

Output example – 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=3722 (wrapped)]

3721 2008/02/07 09:14:06.69 UTC WARNING: SYSTEM #2006 Base LOGGER
"Log File Id 2 configuration modified"

3720 2008/02/07 09:13:18.86 UTC WARNING: SYSTEM #2006 Base LOGGER
"Log File Id 2 configuration modified"

3719 2008/02/01 11:54:15.67 UTC MINOR: IP #2004 management PIP MANAGEMENT
"ARP information overwritten for 10.120.52.253 by 00:e0:52:d4:a5:00"

3718 2008/02/01 11:54:15.40 UTC MINOR: IP #2004 management PIP MANAGEMENT
"ARP information overwritten for 10.120.52.253 by 00:e0:5e:00:a5:00"
...
===============================================================================
A:gal171
```

snmp-trap-group

Syntax

snmp-trap-group [*log-id*]

Context

show>log

Description

This command displays SNMP trap group configuration information.

Parameters

log-id

displays only SNMP trap group information for the specified trap group log ID

Values 1 to 100

Output

The following output is an example of SNMP trap group information, and Table 55: SNMP trap group field descriptions describes the fields.

Output example

```
*A:ALU-48>config>log# show log snmp-trap-group
===============================================================================
SNMP Trap Groups
===============================================================================
id        name
  port      address
-------------------------------------------------------------------------------
29        name
  162       10.20.30.10
===============================================================================
*A:ALU-48>config>log#
```

```
*A:ALU-48>config>log# show log snmp-trap-group 90
===============================================================================
SNMP Trap Group 90
===============================================================================
Description   : none
-------------------------------------------------------------------------------
Name          : 10.121.107.98:162
Address       : 10.121.107.98
Port          : 162
Version       : v2c
Community     : private
Sec. Level    : none
Replay        : disabled
First replay  : n/a
Last replay   : never
===============================================================================
*A:ALU-48>config>log#
```

Table 55: SNMP trap group field descriptions

Label	Description
Name	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 v1, v2c, and v3.
Community	The community string required by snmpv1 or snmpv2c trap receivers
Sec. Level	The required authentication and privacy security levels required to access the views on this node

Label	Description
Replay	Indicates whether the replay parameter has been configured for the trap-target address: enabled or disabled
First replay	Indicates the sequence ID of the first missed notification that will be replayed when a route by which the trap-target address can be reached is added to the routing table. If no notifications are waiting to be replayed, this field shows "n/a".
Last replay	Indicates the last time that missed events were replayed to the trap-target address. If no events have ever been replayed, this field shows "never".

syslog

Syntax

syslog [*syslog-id*]

Context

show>log

Description

This command displays syslog event log destination summary information or detailed information for a specific syslog destination.

Parameters

syslog-id

displays detailed information for the specified syslog event log destination

Values 1 to 10

Output

The following output is an example of syslog event log destination summary information, and Table 56: Syslog field descriptions describes the fields.

Output example

```
*A:ALU-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                                               mail        yes
===============================================================================
```

```
*A:ALU-48>config>log#
```

```
*A:ALU-48>config>log# show log syslog 1
===============================================================================
Syslog Target 1
===============================================================================
IP Address       : 192.168.15.22
Port             : 514
Log-ids          : none
Prefix           : Sr12
Facility         : mail
Severity Level   : info
Prefix Level     : yes
Below Level Drop : 0
Description      : Linux Station Springsteen
===============================================================================
*A:ALU-48>config>log#
```

Table 56: Syslog field descriptions

Label	Description
Syslog ID	The syslog ID number for the syslog destination
IP Address	The IP address of the syslog target host
Port	The configured UDP port number used when sending syslog messages
Facility	The facility code for messages sent to the syslog target host
Severity Level	The syslog message severity level threshold
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.
Prefix Present	Yes: a log prefix was prepended to the syslog message sent to the syslog host
	No: a log prefix was not prepended to the syslog message sent to the syslog host
Description	A text description stored in the configuration file for a configuration context
LogPrefix	The prefix string prepended to the syslog message
Log-id	Events are directed to this destination

5.12.2.3 Clear commands

log-id

Syntax

log-id *log-id*

Context

clear>log

Description

This command reinitializes or rolls over the specified memory log or log file. Memory logs are reinitialized and cleared of contents. Log files are manually rolled over.

This command is only applicable to event logs that are directed to file destinations and memory destinations.

SNMP, syslog, and console/session logs are not affected by this command.

Parameters

log-id

the event log ID to be reinitialized or rolled over

Values 1 to 100

event-handling

Syntax

event-handling

Context

clear>log

Description

This command enables the context to clear Event Handling System (EHS) information.

handler

Syntax

handler *event-handler-name*

Context

clear>log>event-handling

Description

This command clears the event-handler statistics for the specified event handler. These statistics are displayed in the **show log event-handling handler** *handler-name* output. The command does not clear the global or aggregate event-handling statistics.

Parameters

event-handler-name

the name of the event handler

information

Syntax

information

Context

clear>log>event-handling

Description

This command clears global and aggregate event-handling statistics. These statistics are displayed in the **show log event-handling information** output.

6 List of acronyms

Table 57: Acronyms

Acronym	Expansion
2G	second-generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third-generation mobile telephone technology
6VPE	IPv6 on virtual private edge router
7705 SAR	7705 Service Aggregation Router
7750 SR	7750 Service Router
8 PSK	eight phase shift keying
16 QAM	16-state quadrature amplitude modulation
32 QAM	32-state quadrature amplitude modulation
64 QAM	64-state quadrature amplitude modulation
128 QAM	128-state quadrature amplitude modulation
256 QAM	256-state quadrature amplitude modulation
ABR	area border router available bit rate
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
AD	auto-discovery
ADM	add/drop multiplexer
ADP	automatic discovery protocol
AES	advanced encryption standard
AFI	authority and format identifier

Acronym	Expansion
AIGP	accumulated IGP
AIS	alarm indication signal
ALG	application level gateway
AMP	active multipath
AN	association number
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system
ASAP	any service, any port
ASBR	autonomous system boundary router
ASM	any-source multicast autonomous system message
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
AU	administrative unit
AUG	administrative unit group
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
BBE	background block errors
Bc	committed burst size
Be	excess burst size
BECN	backward explicit congestion notification
Bellcore	Bell Communications Research

Acronym	Expansion
BFD	bidirectional forwarding detection
BGP	border gateway protocol
BGP-LS	border gateway protocol link state
BGP-LU	border gateway protocol labeled unicast
BITS	building integrated timing supply
BTCA	best timeTransmitter clock algorithm
BMU	broadcast, multicast, and unknown traffic Traffic that is not unicast. Any nature of multipoint traffic: • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BNM	bandwidth notification message
BOF	boot options file
BoS	bottom of stack
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSM	bootstrap message
BSR	bootstrap router
BSTA	Broadband Service Termination Architecture
BTS	base transceiver station
CA	certificate authority connectivity association
CAK	connectivity association key
CAS	channel associated signaling

Acronym	Expansion
CBN	common bonding networks
CBS	committed buffer space
CC	continuity check control channel
CCM	continuity check message
CCTV	closed-circuit television
CE	circuit emulation customer edge
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
cHDLC	Cisco high-level data link control protocol
CIDR	classless inter-domain routing
CIR	committed information rate
CKN	connectivity association key name
CLI	command line interface
CLP	cell loss priority
CMP	certificate management protocol
C-multicast	customer multicast
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPROTO	C prototype
CPU	central processing unit

Acronym	Expansion
C/R	command/response
CRC	cyclic redundancy check
CRC-32	32-bit cyclic redundancy check
CRL	certificate revocation list
CRON	a time-based scheduling service (from chronos = time)
CRP	candidate RP
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-tag	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
CWDM	coarse wavelength-division multiplexing
DA/FAN	distribution automation and field area network
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DCR	differential clock recovery
DDoS	distributed DoS
DE	discard eligibility
DER	distinguished encoding rules
DES	data encryption standard
DF	do not fragment designated forwarder
DH	Diffie-Hellman

Acronym	Expansion
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6
DIS	designated intermediate system
DLCI	data link connection identifier
DLCMI	data link connection management interface
DM	delay measurement
DNS	domain name server
DNU	do not use
DoS	denial of service
dot1p	IEEE 802.1p bits, in Ethernet or VLAN ingress packet headers, used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPD	dead peer detection
DPI	deep packet inspection
DPLL	digital phase locked loop
DR	designated router
DSA	digital signal algorithm
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DUS	do not use for synchronization
DV	delay variation
DVMRP	distance vector multicast routing protocol
e911	enhanced 911 service

Acronym	Expansion
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)
E-BSR	elected BSR
ECMP	equal cost multipath
EE	end entity
EFM	Ethernet in the first mile
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
EIR	excess information rate
EJBCA	Enterprise Java Beans Certificate Authority
E-LAN	Ethernet local area network
E-Line	Ethernet virtual private line
EL	entropy label
eLER	egress label edge router
ELI	entropy label indicator
E&M	ear and mouth earth and magneto exchange and multiplexer
eMBMS	evolved MBMS
EOP	end of packet
EPC	evolved packet core
EPD	early packet discard
Epipe	Ethernet VLL
EPL	Ethernet private line
EPON	Ethernet Passive Optical Network
EPS	equipment protection switching

Acronym	Expansion
ERO	explicit route object
ES	Ethernet segment errored seconds
ESD	electrostatic discharge
ESI	Ethernet segment identifier
ESMC	Ethernet synchronization message channel
ESN	extended sequence number
ESP	encapsulating security payload
ESPI	encapsulating security payload identifier
ETE	end-to-end
ETH-BN	Ethernet bandwidth notification
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVC	Ethernet virtual connection
EVDO	evolution - data optimized
EVI	EVPN instance
EVPL	Ethernet virtual private link
EVPN	Ethernet virtual private network
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FD	frequency diversity
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FECN	forward explicit congestion notification
FeGW	far-end gateway
FEP	front-end processor

Acronym	Expansion
FF	fixed filter
FFD	fast fault detection
FIB	forwarding information base
FIFO	first in, first out
FIPS-140-2	Federal Information Processing Standard publication 140-2
FM	fault management
FNG	fault notification generator
FOM	figure of merit
Fpipe	frame relay VLL
FQDN	fully qualified domain name
FR	frame relay
FRG bit	fragmentation bit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
FXO	foreign exchange office
FXS	foreign exchange subscriber
GFP	generic framing procedure
GigE	Gigabit Ethernet
GLONASS	Global Navigation Satellite System (Russia)
GNSS	global navigation satellite system (generic)
GPON	Gigabit Passive Optical Network
GPRS	general packet radio service
GPS	Global Positioning System
GRE	generic routing encapsulation
GRT	global routing table
GSM	Global System for Mobile Communications (2G)

Acronym	Expansion
GTP-U	GPRS tunneling protocol user plane
GW	gateway
HA	high availability
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HDLC	high-level data link control protocol
HEC	header error control
HMAC	hash message authentication code
Hpipe	HDLC VLL
H-QoS	hierarchical quality of service
HSB	hot standby
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
H-VPLS	hierarchical virtual private line service
IANA	Internet Assigned Numbers Authority
IBN	isolated bonding networks
ICB	inter-chassis backup
ICK	integrity connection value key
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
ICV	integrity connection value
IDS	intrusion detection system
IDU	indoor unit
IED	intelligent end device
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008

Acronym	Expansion
IES	Internet enhanced service
IETF	Internet Engineering Task Force
IGMP	Internet group management protocol
IGP	interior gateway protocol
IID	instance ID
IKE	Internet key exchange
iLER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IMET-IR	inclusive multicast Ethernet tag—ingress replication
INVARP	inverse address resolution protocol
IOM	input/output module
IP	Internet protocol
IPCP	Internet protocol control protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
I-PMSI	inclusive PMSI
IPoATM	IP over ATM
IPS	intrusion prevention system
IPSec	Internet protocol security
IR	ingress replication
IRB	integrated routing and bridging
ISA	integrated services adapter
ISAKMP	Internet security association and key management protocol
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization

Acronym	Expansion
IW	interworking
JP	join prune
KEK	key encryption key
KG	key group
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LFA	loop-free alternate
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LMI	local management interface
LOS	line-of-sight loss of signal
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSPA	LSP attributes

Acronym	Expansion
LSR	label switching router link-state request
LSU	link-state update
LT	linktrace
LTE	long term evolution line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE
LTR	link trace reply
MA	maintenance association
MAC	media access control
MACsec	media access control security
MA-ID	maintenance association identifier
MBB	make-before-break
MBGP	multicast BGP multiprotocol BGP multiprotocol extensions for BGP
MBMS	multimedia broadcast multicast service
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MCAC	multicast connection admission control
MC-APS	multi-chassis automatic protection switching
MC-MLPPP	multiclass multilink point-to-point protocol
MCS	multicast server multi-chassis synchronization
MCT	MPT craft terminal
MD	maintenance domain

Acronym	Expansion
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDB	multidrop data bridge
MDL	maintenance data link
MDT	multicast distribution tree
ME	maintenance entity
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association endpoint
MFC	multi-field classification
MHD	multi-homed device
MHF	MIP half function
MHN	multi-homed network
MI	member identifier
MIB	management information base
MI-IS-IS	multi-instance IS-IS
MIR	minimum information rate
MKA	MACsec key agreement
MLD	multicast listener discovery
mLDP	multicast LDP
MLPPP	multilink point-to-point protocol
mLSP	multicast LSP
MoFRR	multicast-only fast reroute
MP	merge point multilink protocol

Acronym	Expansion
	multipoint
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPLSCP	multiprotocol label switching control protocol
MPP	MPT protection protocol
MPR	see Wavence
MPR-e	Microwave Packet Radio (standalone mode)
MPT-HC V2/9558HC	Microwave Packet Transport, High Capacity version 2
MPT-HLC	Microwave Packet Transport, High-Capacity Long-Haul Cubic (ANSI)
MPT-HQAM	Microwave Packet Transport, High Capacity (MPT-HC-QAM) or Extended Power (MPT-XP-QAM) with 512/1024 QAM
MPT-MC	Microwave Packet Transport, Medium Capacity
MPT-XP	Microwave Packet Transport, High Capacity (very high power version of MPT-HC V2/9558HC)
MRAI	minimum route advertisement interval
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDP	Multicast Source Discovery Protocol
MSDU	MAC Service Data Unit
MSK	master session key
MSO	multi-system operator
MS-PW	multi-segment pseudowire
MSS	maximum segment size Microwave Service Switch
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit

Acronym	Expansion
M-VPLS	management virtual private line service
MVPN	multicast VPN
MVR	multicast VPLS registration
MW	microwave
MWA	microwave awareness
N·m	newton meter
NAT	network address translation
NAT-T	network address translation traversal
NBMA	non-broadcast multiple access (network)
ND	neighbor discovery
NE	network element
NET	network entity title
NFM-P	Network Functions Manager - Packet (formerly 5620 SAM)
NGE	network group encryption
NG-MVPN	next generation MVPN
NH	next hop
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLOS	non-line-of-sight
NLPID	network level protocol identifier
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NOC	network operations center
NPAT	network port address translation
NRC-F	Network Resource Controller - Flow

Acronym	Expansion
NRC-P	Network Resource Controller - Packet
NRC-T	Network Resource Controller - Transport
NRC-X	Network Resource Controller - Cross Domain
NSAP	network service access point
NSD	Network Services Director
NSP	native service processing Network Services Platform
NSSA	not-so-stubby area
NTP	Network Time Protocol
NTR	network timing reference
OADM	optical add/drop multiplexer
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier level 3
OCSP	online certificate status protocol
ODU	outdoor unit
OIF	outgoing interface
OLT	optical line termination
OMC	optical management console
ONT	optical network terminal
OOB	out-of-band
OPX	off premises extension
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	open shortest path first
OSPF-TE	OSPF-traffic engineering (extensions)

Acronym	Expansion
OSS	operations support system
OSSP	organization specific slow protocol
OTP	one time password
OWAMP	one-way active measurement protocol
P2MP	point to multipoint
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities
PSB	path state block
PBO	packet byte offset
PBR	policy-based routing
PBX	private branch exchange
PCAP	packet capture
PCC	path computation client
PCE	path computation element
PCEP	Path Computation Element Communication Protocol
PCM	pulse code modulation
PCP	priority code point
PCR	proprietary clock recovery
PDU	power distribution unit protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PEAPv0	protected extensible authentication protocol version 0
PEM	privacy enhanced mail
PFoE	power feed over Ethernet
PFS	perfect forward secrecy

Acronym	Expansion
PHB	per-hop behavior
PHP	penultimate hop popping
PHY	physical layer
PIC	prefix independent convergence
PID	protocol ID
PIM SSM	protocol independent multicast—source-specific multicast
PIR	peak information rate
PKCS	public key cryptography standards
PKI	public key infrastructure
PLAR	private line automatic ringdown
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
PLSP	path LSP
PM	performance monitoring
PMSI	P-multicast service interface
P-multicast	provider multicast
PN	packet number
PoE	power over Ethernet
PoE+	power over Ethernet plus
POH	path overhead
POI	purge originator identification
PoP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PPS	pulses per second
PRC	primary reference clock

Acronym	Expansion
PRS	primary reference source
PRTC	primary reference time clock
PSE	power sourcing equipment
PSK	pre-shared key
PSN	packet switched network
PSNP	partial sequence number PDU
PTA	PMSI tunnel attribute
PTM	packet transfer mode
PTP	performance transparency protocol Precision Time Protocol
PuTTY	an open-source terminal emulator, serial console, and network file transfer application
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
Q.922	ITU-T Q-series Specification 922
QL	quality level
QoS	quality of service
QPSK	quadrature phase shift keying
RADIUS	Remote Authentication Dial In User Service
RAN	radio access network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication
RED	random early discard
RESV	reservation

Acronym	Expansion
RIB	routing information base
RIP	routing information protocol
RJ45	registered jack 45
RMON	remote network monitoring
RNC	radio network controller
RP	rendezvous point
RPF RTM	reverse path forwarding RTM
RPS	radio protection switching
RPT	rendezvous-point tree
RR	route reflector
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSA	Rivest, Shamir, and Adleman (authors of the RSA encryption algorithm)
RSHG	residential split horizon group
RSTP	rapid spanning tree protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit
RTC	route target constraint
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
r-VPLS	routed virtual private LAN service
SA	security association source-active

Acronym	Expansion
SAA	service assurance agent
SAFI	subsequent address family identifier
SAK	security association key
SAP	service access point
SAToP	structure-agnostic TDM over packet
SCADA	supervisory control and data acquisition
SC-APS	single-chassis automatic protection switching
SCI	secure channel identifier
SCP	secure copy
SCTP	Stream Control Transmission Protocol
SD	signal degrade space diversity
SDH	synchronous digital hierarchy
SDI	serial data interface
SDN	software defined network
SDP	service destination point
SE	shared explicit
SeGW	secure gateway
SES	severely errored seconds
SETS	synchronous equipment timing source
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SFTP	SSH file transfer protocol
(S,G)	(source, group)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate

Acronym	Expansion
SL	short length
SLA	service-level agreement
SLARP	serial line address resolution protocol
SLID	subscriber location identifier of a GPON module
SLM	synthetic loss measurement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNR	signal to noise ratio
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first
SPI	security parameter index
S-PMSI	selective PMSI
SPT	shortest path tree
SR	Service Router (7750 SR) segment routing
SRLG	shared risk link group
SRP	stateful request parameter
SRRP	subscriber routed redundancy protocol
SR-ISIS	segment routing IS-IS
SR-OSPF	segment routing OSPF
SR-TE	segment routing traffic engineering
SSH	secure shell
SSM	source-specific multicast synchronization status messaging
SSU	system synchronization unit
S-tag	service VLAN tag

Acronym	Expansion
STM	synchronous transport module
STM1	synchronous transport module, level 1
STP	spanning tree protocol
STS	synchronous transport signal
SVC	switched virtual circuit
SVEC	synchronization vector
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCI	tag control information
TCP	transmission control protocol
TDA	transmit diversity antenna
TDEV	time deviation
TDM	time division multiplexing
TE	traffic engineering
TEDB	traffic engineering database
TEID	tunnel endpoint identifier
TEP	tunnel endpoint
TFTP	trivial file transfer protocol
T-LDP	targeted LDP
TLS	transport layer security
TLV	type length value
TM	traffic management
ToD	time of day
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier

Acronym	Expansion
TPIF	IEEE C37.94 teleprotection interface
TPMR	two-port MAC relay
TPS	transmission protection switching
TSoP	transparent SDH/SONET over packet
TTL	time to live
TTLS	tunneled transport layer security
TTM	tunnel table manager
TU	tributary unit
TUG	tributary unit group
TWAMP	two-way active measurement protocol
U-APS	unidirectional automatic protection switching
UAS	unavailable seconds
UBR	unspecified bit rate
UDP	user datagram protocol
UFD	unidirectional forwarding detection
UMH	upstream multicast hop
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
uRPF	unicast reverse path forwarding
V.11	ITU-T V-series Recommendation 11
V.24	ITU-T V-series Recommendation 24
V.35	ITU-T V-series Recommendation 35
VC	virtual circuit
VCB	voice conference bridge
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier

Acronym	Expansion
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VM	virtual machine
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VPWS	virtual private wire service
VRF	virtual routing and forwarding table
VRRP	virtual router redundancy protocol
V-SAP	virtual service access point
VSE	vendor-specific extension
VSI	virtual switch instance
VSO	vendor-specific option
VT	virtual trunk virtual tributary
VTG	virtual tributary group
Wavence	formerly 9500 MPR (Microwave Packet Radio)
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard
WTR	wait to restore
X.21	ITU-T X-series Recommendation 21

Acronym	Expansion
XOR	exclusive-OR
XRO	exclude route object

7 Supported standards and protocols

This chapter lists the 7705 SAR compliance with security and telecom standards, the protocols supported, and proprietary MIBs.

7.1 Security standards

FIPS 140-2—Federal Information Processing Standard publication 140-2, Security Requirements for Cryptographic Modules

7.2 Telecom standards

ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

IEEE 802.1AB-2016—IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery

IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks–Virtual Bridged Local Area Networks

IEEE Std 802.1AE-2006 Media Access Control (MAC) Security

IEEE Std 802.1AEbw-2013—Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering

IEEE 802.1ag—Service Layer OAM

IEEE 802.1p/q—VLAN Tagging

IEEE 802.1x-2010—IEEE Standard for Local and Metropolitan Area Networks–Port-based Network Access Control

IEEE 802.3—10BaseT

IEEE 802.3ab—1000BaseT

IEEE 802.3ah—Ethernet OAM

IEEE 802.3u—100BaseTX

IEEE 802.3x —Flow Control

IEEE 802.3z—1000BaseSX/LX

IEEE 802.3-2008—Revised base standard

IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)

IEEE C37.94-2017—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment

ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)

ITU-T G.826—End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

ITU-T G.8032 — Ethernet Ring Protection Switching

ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics

ITU-T Y.1564—Ethernet service activation test methodology

ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

7.3 Protocol support

7.3.1 ATM

AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)

af-tm-0121.000—Traffic Management Specification Version 4.1, March 1999

GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996

ITU-T Recommendation I.432.1—B-ISDN user-network interface - Physical layer specification: General characteristics

ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95

RFC 2514—Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999

RFC 2515—Definition of Managed Objects for ATM Management, February 1999

RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5

7.3.2 BFD

RFC 7130—Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces

RFC 7881—Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS

draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base

draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection

draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)

draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

7.3.3 BGP

RFC 1397—BGP Default Route Advertisement

RFC 1997—BGP Communities Attribute

RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option

RFC 2439—BGP Route Flap Dampening

RFC 2545—Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing

RFC 2918—Route Refresh Capability for BGP-4

RFC 3107—Carrying Label Information in BGP-4

RFC 3392—Capabilities Advertisement with BGP-4

RFC 4271—BGP-4 (previously RFC 1771)

RFC 4360—BGP Extended Communities Attribute

RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)

RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)

RFC 4486—Subcodes for BGP Cease Notification Message

RFC 4684—Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)

RFC 4724—Graceful Restart Mechanism for BGP - GR Helper

RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)

RFC 4893—BGP Support for Four-octet AS Number Space

RFC 4798—Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)

RFC 5549—Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop

RFC 6513—Multicast in MPLS/BGP IP VPNs

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

RFC 7311—The Accumulated IGP Metric Attribute for BGP

RFC 7606—Revised Error Handling for BGP UPDATE Messages

draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP

draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of Multiple Paths in BGP

7.3.4 DHCP/DHCPv6

RFC 1534—Interoperation between DHCP and BOOTP

RFC 2131—Dynamic Host Configuration Protocol (REV)

RFC 2132—DHCP Options and BOOTP Vendor Extensions

RFC 3046—DHCP Relay Agent Information Option (Option 82)

RFC 3315—Dynamic Host Configuration Protocol for IPv6

RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

7.3.5 Differentiated services

RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers

RFC 2597—Assured Forwarding PHB Group

RFC 2598—An Expedited Forwarding PHB

RFC 3140—Per-Hop Behavior Identification Codes

7.3.6 Digital data network management

V.35

RS-232 (also known as EIA/TIA-232)

X.21

7.3.7 ECMP

RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

7.3.8 Ethernet VPN (EVPN)

RFC 7432—BGP MPLS-Based Ethernet VPN

draft-ietf-bess-evpn-vpls-seamless-integ—(PBB-)EVPN Seamless Integration with (PBB-)VPLS

draft-ietf-bess-evpn-vpws—Virtual Private Wire Service support in Ethernet VPN

draft-ietf-rabadan-bess-evpn-pref-pdf—Preference-based EVPN DF Election

7.3.9 Frame relay

ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service

ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer - ISDN data link layer specification for frame mode bearer services

FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement

RFC 2427—Multiprotocol Interconnect over Frame Relay

7.3.10 GRE

RFC 2784—Generic Routing Encapsulation (GRE)

7.3.11 Internet protocol (IP) – version 4

RFC 768—User Datagram Protocol

RFC 791—Internet Protocol

RFC 792—Internet Control Message Protocol

RFC 793—Transmission Control Protocol

RFC 826—Ethernet Address Resolution Protocol

RFC 854—Telnet Protocol Specification

RFC 1350—The TFTP Protocol (Rev. 2)

RFC 1812—Requirements for IPv4 Routers

RFC 3021—Using 31-Bit Prefixes on IPv4 Point-to-Point Links

7.3.12 Internet protocol (IP) – version 6

RFC 2460—Internet Protocol, Version 6 (IPv6) Specification

RFC 2462—IPv6 Stateless Address Autoconfiguration

RFC 2464—Transmission of IPv6 Packets over Ethernet Networks

RFC 3587—IPv6 Global Unicast Address Format

RFC 3595—Textual Conventions for IPv6 Flow Label

RFC 4007—IPv6 Scoped Address Architecture

RFC 4193—Unique Local IPv6 Unicast Addresses

RFC 4291—IPv6 Addressing Architecture

RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 4649—DHCPv6 Relay Agent Remote-ID Option

RFC 4861—Neighbor Discovery for IP version 6 (IPv6)

RFC 5095—Deprecation of Type 0 Routing Headers in IPv6

RFC 5952—A Recommendation for IPv6 Address Text Representation

7.3.13 IPSec

ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

PKCS #12 Personal Information Exchange Syntax Standard

RFC 2315—PKCS #7: Cryptographic Message Syntax

RFC 2409—The Internet Key Exchange (IKE)

RFC 2986—PKCS #10: Certification Request Syntax Specification

RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

RFC 3947—Negotiation of NAT-Traversal in the IKE

RFC 3948—UDP Encapsulation of IPsec ESP Packets

RFC 4301—Security Architecture for the Internet Protocol

RFC 4303—IP Encapsulating Security Payload (ESP)

RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 7383—Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation

7.3.14 IS-IS

RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)

RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments

RFC 2763—Dynamic Hostname Exchange for IS-IS

RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS

RFC 2973—IS-IS Mesh Groups

RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

RFC 3567—Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

RFC 3719—Recommendations for Interoperable Networks using IS-IS

RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)

RFC 3787—Recommendations for Interoperable IP Networks

RFC 4205 for Shared Risk Link Group (SRLG) TLV

RFC 4971—Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information

RFC 5120—M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)

RFC 5304—IS-IS Cryptographic Authentication

RFC 5305—IS-IS Extensions for Traffic Engineering

RFC 5307—IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)

RFC 5308—Routing IPv6 with IS-IS

RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols

RFC 5310—IS-IS Generic Cryptographic Authentication

RFC 6232—Purge Originator Identification TLV for IS-IS

7.3.15 LDP

RFC 5036—LDP Specification

RFC 5283—LDP Extension for Inter-Area Label Switched Paths

RFC 5350—-IANA Considerations for the IPv4 and IPv6 Router Alert Options

RFC 5443—LDP IGP Synchronization

RFC 5561—LDP Capabilities

RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root

RFC 6829—Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6

RFC 7552—Updates to LDP for IPv6

draft-ietf-mpls-ldp-ip-pw-capability—Controlling State Advertisements Of Non-negotiated LDP Applications

draft-ietf-mpls-oam-ipv6-rao—IPv6 Router Alert Option for MPLS OAM

draft-pdutta-mpls-ldp-adj-capability-00—LDP Adjacency Capabilities

draft-pdutta-mpls-ldp-v2-00—LDP Version 2

draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multi-point LDP Tunnels

7.3.16 LDP and IP FRR

RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

RFC 7490—Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)

7.3.17 MPLS

RFC 3031—MPLS Architecture

RFC 3032—MPLS Label Stack Encoding

RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)

RFC 5440—Path Computation Element (PCE) Communication Protocol (PCEP)

RFC 6790—The Use of Entropy Labels in MPLS Forwarding

RFC 8253—PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)

RFC 8697—Path Computation Element Communication Protocol (PCEP) Extensions for Establishing Relationships between Sets of Label Switched Paths (LSPs)

RFC 8745—Path Computation Element Communication Protocol (PCEP) Extensions for Associating Working and Protection Label Switched Paths (LSPs) with Stateful PCE

RFC 8800—Path Computation Element Communication Protocol (PCEP) Extension for Label Switched Path (LSP) Diversity Constraint Signaling

draft-dhody-pce-pceps-tls13-02—Updates for PCEPS

draft-ietf-pce-stateful-pce—PCEP Extensions for Stateful PCE

draft-ietf-pce-segment-routing—PCEP Extensions for Segment Routing

draft-alvarez-pce-path-profiles—PCE Path Profiles

7.3.18 MPLS – OAM

RFC 6424— Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

RFC 8029—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

7.3.19 Multicast

RFC 3956—Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

RFC 3973—Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

RFC 4610—Anycast-RP Using Protocol Independent Multicast (PIM), which is similar to RFC 3446—Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs

RFC 6826—Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

cisco-ipmulticast/pim-autorp-spec—Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast, which is similar to RFC 5059—Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)

draft-ietf-mboned-msdp-deploy-nn.txt—Multicast Source Discovery Protocol (MSDP) Deployment Scenarios

7.3.20 Network management

IANA-IFType-MIB

ITU-T X.721—Information technology- OSI-Structure of Management Information

ITU-T X.734—Information technology- OSI-Systems Management: Event Report Management Function

M.3100/3120—Equipment and Connection Models

RFC 1157—SNMPv1

RFC 1850—OSPF-MIB

RFC 1907—SNMPv2-MIB

RFC 2011—IP-MIB

RFC 2012—TCP-MIB

RFC 2013—UDP-MIB

RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

RFC 2096—IP-FORWARD-MIB

RFC 2138—RADIUS

RFC 2206—RSVP-MIB

RFC 2571—SNMP-FRAMEWORKMIB

RFC 2572—SNMP-MPD-MIB

RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB

RFC 2574—SNMP-USER-BASED-SMMIB

RFC 2575—SNMP-VIEW-BASED ACM-MIB

RFC 2576—SNMP-COMMUNITY-MIB

RFC 2588—SONET-MIB

RFC 2665—EtherLike-MIB

RFC 2819—RMON-MIB

RFC 2863—IF-MIB

RFC 2864—INVERTED-STACK-MIB

RFC 3014—NOTIFICATION-LOG MIB

RFC 3164—The BSD Syslog Protocol

RFC 3273—HCRMON-MIB

RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413—Simple Network Management Protocol (SNMP) Applications

RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3418—SNMP MIB

RFC 3954—Cisco Systems NetFlow Services Export Version 9

RFC 5101—Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information

RFC 5102—Information Model for IP Flow Information Export

draft-ietf-disman-alarm-mib-04.txt

draft-ietf-mpls-ldp-mib-07.txt

draft-ietf-ospf-mib-update-04.txt

draft-ietf-mpls-lsr-mib-06.txt

draft-ietf-mpls-te-mib-04.txt

TMF 509/613—Network Connectivity Model

7.3.21 OSPF

RFC 1765—OSPF Database Overflow

RFC 2328—OSPF Version 2

RFC 2370—Opaque LSA Support

RFC 2740—OSPF for IPv6

RFC 3101—OSPF NSSA Option

RFC 3137—OSPF Stub Router Advertisement

RFC 3509—Alternative Implementations of OSPF Area Border Routers

RFC 3623—Graceful OSPF Restart (support for Helper mode)

RFC 3630—Traffic Engineering (TE) Extensions to OSPF

RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

RFC 4915—Multi-Topology (MT) Routing in OSPF

RFC 4970—Extensions to OSPF for Advertising Optional Router Capabilities

RFC 5185—OSPF Multi-Area Adjacency

7.3.22 OSPFv3

RFC 4552—Authentication/Confidentiality for OSPFv3

7.3.23 PPP

RFC 1332—PPP Internet Protocol Control Protocol (IPCP)

RFC 1570—PPP LCP Extensions

RFC 1619—PPP over SONET/SDH

RFC 1661—The Point-to-Point Protocol (PPP)

RFC 1662—PPP in HDLC-like Framing

RFC 1989—PPP Link Quality Monitoring

RFC 1990—The PPP Multilink Protocol (MP)

RFC 2686—The Multi-Class Extension to Multi-Link PPP

7.3.24 Pseudowires

Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks

RFC 3550—RTP: A Transport Protocol for Real-Time Applications

RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture

RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

RFC 4446—IANA Allocation for PWE3

RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks

RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks

RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks

RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks

RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service

RFC 5085—Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RFC 5086—Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

7.3.25 RIP

RFC 1058—Routing Information Protocol

RFC 2453—RIP Version 2

7.3.26 RADIUS

RFC 2865—Remote Authentication Dial In User Service

RFC 2866—RADIUS Accounting

7.3.27 RSVP-TE and FRR

RFC 2430—A Provider Architecture for DiffServ & TE

RFC 2702—Requirements for Traffic Engineering over MPLS

RFC 2747—RSVP Cryptographic Authentication

RFC 2961—RSVP Refresh Overhead Reduction Extensions

RFC 3097—RSVP Cryptographic Authentication - Updated Message Type Value

RFC 3209—Extensions to RSVP for LSP Tunnels

RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels

RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)

RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels

7.3.28 Segment routing (SR)

draft-francois-rtgwg-segment-routing-ti-lfa-04—Topology Independent Fast Reroute using Segment Routing

draft-gredler-idr-bgp-ls-segment-routing-ext-03—BGP Link-State extensions for Segment Routing

draft-ietf-isis-segment-routing-extensions-04—IS-IS Extensions for Segment Routing

draft-ietf-mpls-spring-lsp-ping-02—Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane

draft-ietf-ospf-segment-routing-extensions-04—OSPF Extensions for Segment Routing

draft-ietf-spring-segment-routing-15—Segment Routing Architecture

7.3.29 SONET/SDH

GR-253-CORE—SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

ITU-T Recommendation G.841—Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

7.3.30 SSH

RFC 4253—The Secure Shell (SSH) Transport Layer Protocol

draft-ietf-secsh-architecture.txt—SSH Protocol Architecture

draft-ietf-secsh-userauth.txt—SSH Authentication Protocol

draft-ietf-secsh-connection.txt—SSH Connection Protocol

draft-ietf-secsh- newmodes.txt—SSH Transport Layer Encryption Modes

draft-ietf-secsh-filexfer-13.txt—SSH File Transfer Protocol

7.3.31 Synchronization

G.781—Synchronization layer functions, 2001/09/17

G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813—Timing characteristics of SDH equipment slave clocks (SEC)

G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16

G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16

G.8261—Timing and synchronization aspects in packet networks

G.8262—Timing characteristics of synchronous Ethernet equipment slave clock

GR 1244 CORE—Clocks for the Synchronized Network: Common Generic Criteria

IEC/IEEE 61850-9-3—Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation

IEEE C37.238-2017 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, Annex E – Transport of PTP over User Datagram Protocol over Internet Protocol Version 6

IEEE Std 1588-2019—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, Annex J

ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008

ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010

ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014

ITU-T G.8275.2—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for time/phase synchronization with partial timing support from the network, issued 06/2016

RFC 5905—Network Time Protocol Version 4: Protocol and Algorithms Specification

7.3.32 TACACS+

IETF draft-grant-tacacs-02.txt—The TACACS+ Protocol

7.3.33 TLS

RFC 5246—The Transport Layer Security (TLS) Protocol Version 1.2

RFC 5922—Domain Certificates in the Session Initiation Protocol (SIP)

RFC 6460—Suite B Profile for Transport Layer Security (TLS)

RFC 8446—The Transport Layer Security (TLS) Protocol Version 1.3

7.3.34 TWAMP

RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

7.3.35 VPLS

RFC 4762—Virtual Private LAN Services Using LDP

7.3.36 VRRP

RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol

RFC 3768 Virtual Router Redundancy Protocol

RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

7.4 Proprietary MIBs

TIMETRA-ATM-MIB.mib

TIMETRA-CAPABILITY-7705-V1.mib

TIMETRA-CHASSIS-MIB.mib

TIMETRA-CLEAR-MIB.mib

TIMETRA-FILTER-MIB.mib

TIMETRA-GLOBAL-MIB.mib

TIMETRA-LAG-MIB.mib

TIMETRA-LDP-MIB.mib

TIMETRA-LOG-MIB.mib

TIMETRA-MPLS-MIB.mib

TIMETRA-OAM-TEST-MIB.mib

TIMETRA-PORT-MIB.mib

TIMETRA-PPP-MIB.mib

TIMETRA-QOS-MIB.mib

TIMETRA-ROUTE-POLICY-MIB.mib

TIMETRA-RSVP-MIB.mib

TIMETRA-SAP-MIB.mib

TIMETRA-SDP-MIB.mib

TIMETRA-SECURITY-MIB.mib

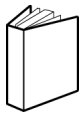
TIMETRA-SERV-MIB.mib

TIMETRA-SYSTEM-MIB.mib

TIMETRA-TC-MIB.mib

TIMETRA-VRRP-MIB.mib

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback