7750 SR OS
System Management Guide

Software Version: 7750 SR OS 10.0 R1
February 2012
Document Part Number: 93-0071-09-01

Table of Contents

SNMP

Event and Accounting Logs

Facility Alarms

List of Tables

Getting Started

Security

SNMP

Event and Accounting Logs

Facility Alarms

LIST OF FIGURES

Security

SNMP

Event and Accounting Logs

Facility Alarms

Preface

About This Guide

This guide describes the services and protocol support provided by the 7750 SR OSand presents examples to configure and implement MPLS, RSVP, and LDP protocols.

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

Audience

This manual is intended for network administrators who are responsible for configuring the 7750 SR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols and concepts described in this manual include the following:

- Multiprotocol Label Switching (MPLS)
- Resource Reservation Protocol (RSVP)
- Label Distribution Protocol (LDP)

List of Technical Publications

The 7750 SR documentation set is composed of the following books:

- 7750 SR OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7750 SR OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), MCM (MDA Carrier Module), CMA (Compact Media Adapter), and port provisioning.

- 7750 SR OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering, and VRRP, and Cflowd and Cflowd.

- 7750 SR OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, Multicast, BGP, Multicast, BGP, and route policies.

- 7750 SR OS MPLS Guide

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

- 7750 SR OS Services Guide

  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.

- 7750 SR OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- 7750 SR OS Triple Play Guide

  This guide describes Triple Play services and support provided by the 7750 SR7450 ESS7710 SR and presents examples to configure and implement various protocols and services.

- 7750 SR OS Quality of Service Guide

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

- OS Multi-Service ISA Guide

  This guide describes services provided by integrated service adapters such as Application Assurance, IPSec, ad insertion (ADI) and Network Address Translation (NAT).

Technical Support

If you purchased a service agreement for your 7750 SR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center:

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

Getting Started

In This Chapter

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

Alcatel-Lucent 7750 SR Router Configuration Process

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

Table 1: Configuration Process

Area	Task	Chapter
System security	Configure system security parameters, such as authentication, authorization, and accounting.	Security on page 19
Network management	Configure SNMP elements.	SNMP on page 251
Operational functions	Configure event and accounting logs.	Event and Accounting Logs on page 301
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 485

Security

In This Chapter

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

Authentication, Authorization, and Accounting

This chapter describes authentication, authorization, and accounting (AAA) used to monitor and control network access on 7750 SR-Series routers. Network security is based on a multi-step process. The first step, authentication, validates a user's name and password. The second step is authorization, which allows the user to access and execute commands at various command levels based on profiles assigned to the user.

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

You can configure 7750 SR-Series routers to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, or FTP. You can select the authentication order which determines the authentication method to try first, second, and third.

7750 SR OS supports the following security features:

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

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

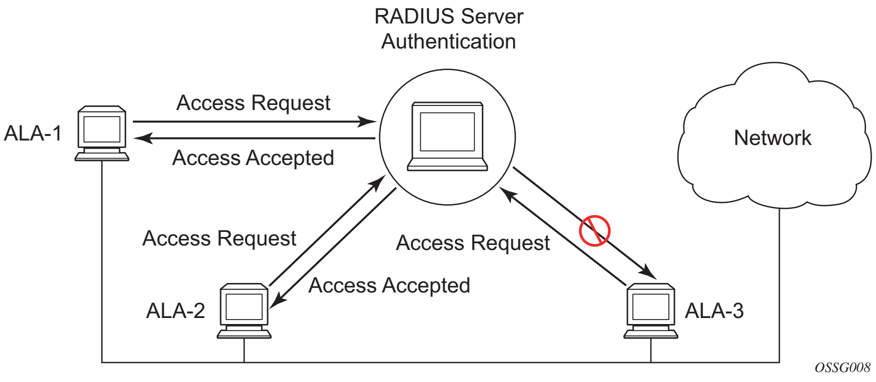

Figure 1: RADIUS Requests and Responses

Authentication

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

When a user attempts to log in through the console, Telnet, SSH, SCP, or FTP, the 7750 SR-Series client sends an access request to a RADIUS, TACACS+, or local database.

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

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

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

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

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

Implementing authentication without authorization for the 7750 SR-Seriesrouters 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 7750 SR-Series router:

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

Local Authentication

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

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

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

RADIUS Authentication

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

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

RADIUS Server Selection

The RADIUS server selection algorithm is used by different applications:

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

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

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

Direct Mode

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

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

Round-Robin Mode

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

Server Reachability Detection

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

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

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

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

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

Application Specific Behavior

Operator Management

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

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

RADIUS Authentication

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

RADIUS Accounting

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

RADIUS PE-Discovery

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

The RADIUS PE-discovery application makes use of a 10 second time period instead of the generic 30 seconds and uses a fixed consecutive timeout value of 2 (see Server Reachability Detection on page 23).

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

TACACS+ Authentication

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

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

Authorization

7750 SR-Series routers support local, RADIUS, and TACACS+ authorization to control the actions of specific users by applying a profile based on user name and password configurations once network access is granted. The profiles are configured locally as well as VSAs on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 38.

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

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

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

Profiles must be created on each 7750 SR-Series router and should be identical for consistent results. If the profile is not present, then access is denied.

Table 2 displays the following scenarios:

- Remote (RADIUS) authorization cannot be performed if authentication is done locally (on the 7750 SR-Series router).
- The reverse scenario is supported if RADIUS authentication is successful and no authorization is configured for the user on the RADIUS server, then local (router) authorization is attempted, if configured in the authorization order.

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

Table 2: Supported Authorization Configurations

	7750 SR	RADIUS Supplied Profile
7750 SR-Series configured user	Supported	Not Supported
RADIUS server configured user	Supported	Supported
TACACS+ server configured user	Supported	Not Supported

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

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

Local Authorization

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

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

You must configure profile and user access information locally.

RADIUS Authorization

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

TACACS+ Authorization

Like RADIUS authorization, TACACS+ grants or denies access permissions for a 7750 SR-Series router. The TACACS+ server sends a response based on the username and password.

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

Accounting

When enabled, RADIUS accounting sends command line accounting from the 7750 SR-Series router to the RADIUS server. The router sends accounting records using UDP packets at port 1813 (decimal).

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

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

RADIUS Accounting

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

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

TACACS+ Accounting

7750 SR OS allows you to configure the type of accounting record packet that is to be sent to the TACACS+ server when specified events occur on the device. The accounting **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent. Start/stop messages are only sent for individual commands, not for the session.

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

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

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

Security Controls

You can configure 7750 SR-Series routers to use RADIUS, TACACS+, and local authentication to validate users requesting access to the network. The order in which password authentication is processed among RADIUS, TACACS+ and local passwords can be specifically configured. In other words, the authentication order can be configured to process authorization through TACACS+ first, then RADIUS for authentication and accounting. Local access can be specified next in the authentication order in the event that the RADIUS and TACACS+ servers are not operational.

Table 3: Security Methods Capabilities

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

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

When a Server Does Not Respond

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

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

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

Access Request Flow

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

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

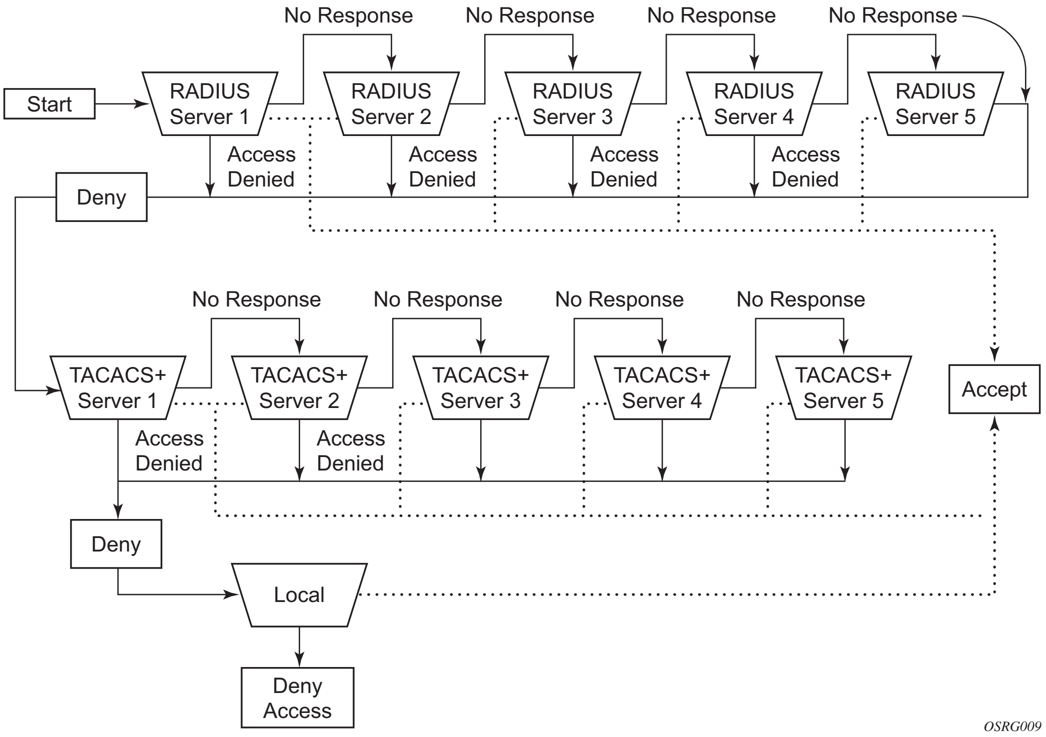

Figure 2: Security Flow

CPU Protection

CPU protection protects the CPU of the node that it is configured on from a DOS attack by limiting the amount of traffic coming in from one of its ports and destined to the CPM (to be processed by its CPU) using a combination of the configurable limits.

Some of the limits are configured globally for the node, and some of the limits are configured in CPU Protection profiles which are assigned to interfaces.

The following limits are configured globally for the node:

- link-specific rate — Applies to the link-specific protocol LACP (LAG control).The rate is a per-link limit (each link in the system will have LACP packets limited to this rate).
- port-overall-rate – Applies to all control traffic each port.   The rate is a per-port limit (each port in the system will have control traffic destined to the CPM limited to this rate).
- protocol-protection — Blocks network control traffic for unconfigured protocols. If IS-IS is not configured on an IP interface all IS-IS-related traffic will be dropped and not reach the CPU.

The following limits are configured within CPU Protection policies (1-255).   CPU Protection policies are created, configured, and then assigned to interfaces.

- overall-rate — Applies to all control traffic (DHCP only for ip-src-monitoring) destined to the CPM (all sources) received on the interface (only where the policy is applied).   This is a per-interface limit.   Control traffic received above this rate will be discarded.
- per-source-rate — Applies to all control traffic destined to the CPM that is received from the same source (SAP + MAC address or SAP + IP source address) (only where the policy is applied).   This is a per-source limit.
- out-profile-rate – Applies to all control traffic destined to the CPM (all sources) received on the interface (only where the policy is applied).   This is a per-interface limit.   Control traffic received above this rate will be marked as discard eligible and is more likely to be discarded if there is contention for CPU resources.

A three-color marking mechanism uses a green, yellow and red marking function. This allows greater flexibility in how traffic limits are implemented. A CLI command within the DoS protection policy called **out-profile-rate** maps to the boundary between the green (accept) and yellow (mark as discard eligible) regions. The **overall-rate** command marks the boundary between the yellow and red (drop) regions point for the associated policy (Figure 3).

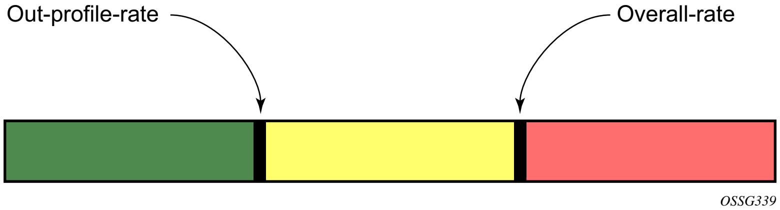

Figure 3: Profile Marking

There are two default CPU protection policies. They are modifiable, but cannot be deleted.

Policy 254:

- This is the default policy that is automatically applied to access interfaces
- Traffic above 6000 pps is discarded
- overall-rate = 6000
- per-source-rate = max
- out-profile-rate = 6000

Policy 255:

- This is the default policy that is automatically applied to Network interfaces
- Traffic above 3000 pps is marked as discard eligible, but is not discarded unless there is congestion in the queueing towards the CPU
- overall-rate = max
- per-source-rate = max
- out-profile-rate = 3000

All traffic destined to the CPM and that will be processed by its CPU will be subject to the limit specified. Therefore, if there is a protocol running on the violating interface, then protocol traffic on that interface will be affected. The objective of CPU protection is to limit the amount of traffic that the CPU will process at an early stage, therefore, the good and bad traffic coming in cannot be distinguished when it arrives at a rate higher than the user-configured limit.

If the overall rate is set to 1000 pps and as long as the total traffic that is destined to the CPM and intended to be processed by the CPU is less than or equal to 1000 pps, all traffic will be processed. If the rate exceeds 1000 pps, then protocol traffic is discarded (or marked as discard eligible in the case of the out-profile-rate) and traffic on the interface is affected.

This protects all the other interfaces on the system and make sure that a violation from one interface does not affect the rest of the box.

The protocol-protection configuration is not a rate (just an enable/disable configuration). When enabled, this feature causes the network processor on the CPM to discard all packets received for protocols that are not configured on the particular interface.   This helps mitigate DoS attacks by filtering invalid control traffic before it hits the CPU.   The system automatically populates and maintains a per-interface list of configured (such as valid) protocols (based on interface config, etc). For example, if an interface does not have IS-IS configured, then protocol-protection will discard any IS-IS packets received on that interface.

Some protocols are not bound to a specific interface , for example, BGP.   SR-OS will discard packets for these protocols if the protocol is not configured anywhere in the system. Note that protection for the following protocols is achieved using the per-peer-queueing feature of SR-OS: BGP, T-LDP, LDP, MSDP, Telnet and SSH.

Protocols controlled by the protocol-protection mechanism include:

- OSPFv2
- OSPFv3
- IS-IS
- RSVP-TE
- RIP
- PIM
- MLD
- IGMP
- BFD
- L2TP
- PPP

Note: If PIM or PIM snooping is not configured on any interfaces/SAPs then all PIM packets will be discarded. If PIM or PIM snooping is configured on an interface/SAP, then multicast PIM messages are filter based on PIM being enabled on that particular interface. All unicast PIM messages are sent to the CPU to be processed.

The CPU protection features are supported on the following platforms:

- 7750 SR-7/SR-12
- 7450 ESS-6/ESS-7/ESS-12

The CPU protection features are **not** supported on the following platforms:

- 7750 SR-1

- 7450 ESS-1
- 7710 SR-c4/c12
- 7750 SR-c4/c12

CPU Protection Extensions ETH-CFM

CPU protection has been extended to provide the ability to explicitly limit the amount of ETH-CFM traffic that arrives at the CPU for processing. ETH-CFM packets that are redirected to the CPU by either a Management Endpoint (MEP) or a Management Intermediate Point (MIP) will be subject to the configured limit of the associated policy. Up to four CPU protection policies may include up to ten individual eth-cfm specific entries. The eth-cfm entries allow the operator to apply a packet per second rate limit to the matching combination of level and opcode, for eth-cfm packet that are redirected to the CPU. Any eth-cfm traffic that is redirected to the CPU by a Management Point (MP) that does not match any entries of the applied policy is still subject to the overall rate limit of the policy itself. Any eth-cfm packets that are not redirected to the CPU are not subject to this function and are treated as transit data, subject to the applicable QoS policy.

The operator first creates a CPU Policy and includes the required eth-cfm entries. Overlap is allowed for the entries within a policy, first match logic is applied. This means ordering the entries in the proper sequence is important to ensure the proper behavior is achieved. Even thought the number of eth-cfm entries is limited to ten, the entry numbers have a valid range from 1-100 to allow for ample space to insert policies between one and other.

Ranges are allowed when configuring the Level and the OpCode. Ranges provide the operator a simplified method for configuring multiple combinations. When more than one Level or OpCode is configured in this manner the configured rate limit is applied separately to each combination of level and OpCode match criteria. For example, if the Levels are configured with using a range of 5-7 and the OpCode is configured for 3,5 with a rate of 1. That restricts all possible combinations on that single entry to a rate of 1 packet per second. In this example six different match conditions are programmed behind the scene.

Table 4: Ranges versus Levels and OpCodes

Level	OpCode	Rate
5	3	1
5	5	1
6	3	1
6	5	1
7	3	1
7	5	1

Once the policy is created it must be applied to a SAP/Binding within a service for these rates to take affect. This means the rate is on a per SAP/Binding basis. Only a single policy may be applied to a SAP/Binding. The “eth-cfm-monitoring” option must be configured in order for the eth-cfm entries to be applied when the policy is applied to the SAP/Binding. If this option is not configured, eth-cfm entries in the policy will be ignored. It is also possible to apply a policy to a SAP/Binding configuring “eth-cfm-monitoring” which does not have an MP. In this case, although these entries are enforced, no packets are being redirect to the CPU due to the lack of an MP.

By default, rates are applied on a per peer basis. This means each individual peer is subject to the rate. However, it is suggested that the “aggregate” option be configured to apply the rate to the sum total of all peers. MIPs for example only respond to Loopback Messages and Linktrace Messages. These are typically on demand functions and per peer rate limiting is likely not required thus making the aggregate function a more appealing model.

“eth-cfm-monitoring” and “mac-monitoring” are mutually exclusive and cannot be configured on the same SAP/Binding. “mac-monitoring” is used in combination with the traditional CPU protection and is not specific to the eth-cfm rate limiting feature describe here.

When an MP is configured on a SAP/Binding within a service which allows an external source to communicate with that MP, for example a User to Network Interface (UNI), it is suggested that “eth-cfm-monitoring” with the “aggregate” option be configured on all SAP/Bindings to provide the highest level of rate control.

The example below shows a sample configuration for a policy and the application of that policy to a SAP in a VPLS service configured with a MP.

Policy 1 entry 10 limits all eth-cfm traffic redirected to the CPU for all possible combinations to 1 packet per second. Policy 1 entry 20 limits all possible combinations to a rate of zero, dropping all request which match any combination. If entry 20 did not exist then only rate limiting of the entry 10 matches would occur and any other eth-cfm packets redirected to the CPU would not be bound by a CPU protection rate.

```
config>sys>security>cpu-protection#
  policy 1
    eth-cfm
      entry 10 level 5-7 opcode 3,5 rate 1
      entry 20 level 0-7 opcode 0-255 rate 0

config>service>vpls#
  sap 1/1/4:100
    cpu-protection 1 eth-cfm-monitoring aggregate
    eth-cfm
      mip
    no shutdown
```

IOM1s are restricted to Down MEPs and ingress MIP for this feature. This feature is not supported on UP MEPs and egress MIPs for this IOM type.

Vendor-Specific Attributes (VSAs)

7750 SR OS software supports the configuration of Alcatel-Lucent-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are discussed in RFC 2138. VSAs must be configured when RADIUS authorization is enabled. It is up to the vendor to specify the format of their VSA. The attribute-specific field is dependent on the vendor's definition of that attribute. The Alcatel-Lucent-defined attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID field set to 6527, the vendor ID number.

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

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

- `timetra-access <ftp> <console> <both>` — This is a mandatory command that must be configured. This command specifies if the user has FTP and /or console (serial port, Telnet, and SSH) access.
- `timetra-profile <profile-name>` — When configuring this VSA for a user, it is assumed that the user profiles are configured on the local 7750 SR-Series router and the following applies for local and remote authentication:

  1. The `authentication-order` parameters configured on the router must include the `local` keyword.
  2. The user name may or may not be configured on the router.
  3. The user must be authenticated by the RADIUS server
  4. Up to 8 valid profiles can exist on the router for a user. The sequence in which the profiles are specified is relevant. The most explicit matching criteria must be ordered first. The process stops when the first complete match is found.

  If all the above mentioned conditions are not met, then access to the router is denied and a failed login event/trap is written to the security log.
- `timetra-default-action <permit-all|deny-all|none>` — This is a mandatory command that must be configured even if the `timetra-cmd` VSA is not used. This command specifies the default action when the user has entered a command and no entry configured in the `timetra-cmd` VSA for the user resulted in a match condition.
- `timetra-cmd <match-string>` — Configures a command or command subtree as the scope for the match condition.

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

Other Security Features

Secure Shell (SSH)

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

7750 SR-Series allows you to configure Secure Shell (SSH) Version 2 (SSH2). SSH1 and SSH2 are different protocols and encrypt at different parts of the packets. SSH1 uses server as well as host keys to authenticate systems whereas SSH2 only uses host keys. SSH2 does not use the same networking implementation that SSH1 does and is considered a more secure, efficient, and portable version of SSH.

SSH runs on top of a transport layer (like TCP or IP), and provides authentication and encryption capabilities.

7750 SR OS has a global SSH server process to support inbound SSH and SCP sessions initiated by external SSH or SCP client applications. The SSH server supports SSHv1. Note that this server process is separate from the SSH and SCP client commands on the routers which initiate outbound SSH and SCP sessions.

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

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

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

When using SCP to copy files from an external device to the file system, the SCP server will accept either forward slash (“/”) or backslash (“\”) characters to delimit directory and/or filenames. Similarly, the SCP client application can use either slash or backslash characters, but not all SCP clients treat backslash characters as equivalent to slash characters. In particular, UNIX systems will often times interpret the backslash character as an “escape” character which does not get transmitted to the SCP server. For example, a destination directory specified as “cf1:\dir1\file1” will be transmitted to the SCP server as “cf1:dir1file1” where the backslash escape characters are stripped by the SCP client system before transmission. On systems where the client treats the backslash like an “escape” character, a double backslash “\\” or the forward slash “/” can typically be used to properly delimit directories and the filename.

Per Peer CPM Queuing

System-level security is crucial in service provider networks to address the increased threat of Denial-of-Service (DoS) attacks.

Control Processor Module Queuing (CPMQ) implements separate hardware-based queues which are allocated on a per-peer basis. CPMQ allocates a separate queue for each LDP and BGP peer and ensures that each queue is served in a round-robin fashion. This mechanism guarantees fair and “non-blocking” access to shared CPU resources across all peers. This would ensure, for example, that an LDP-based DoS attack from a given peer would be mitigated and compartmentalized so that not all CPU resources would be dedicated to the otherwise overwhelming control traffic sent by that specific peer.

CPMQ, using the “per-peer-queuing” command, ensures that service levels would not (or only partially be) impacted in case of an attack from a spoofed LDP or BGP peer IP address.

Per Peer CPM Queueing is supported on the 7750 SR-7/12 and 7750 SR-c12 platforms.   It is not supported on the 7750 SR-1.-1.

CPM Filters and Traffic Management

7750 SR-Series routers have traffic management and queuing hardware dedicated to protecting the control plane. CPM filters are supported on the following platforms: 7750 SR-7/SR-12/SR-c12. CPM queueing is supported on the following platforms: 7750 SR-7/SR-12 and 7750 SR-c12 (not 7750 SR-1).These filters can be used to drop or accept packets, as well as allocate dedicated hardware shaping queues for traffic directed to the control processors.

Users can allocate dedicated CPM hardware queues for certain traffic designated to the CPUs and can set the corresponding rate-limit for the queues.

The following traffic management features are supported:

- Traffic classification using these filters:
  - → Packets going to the CPMare first classified by the IOM into forwarding classes (FCs) before CPM hardware sees them. CPM filters can be used to further classify the packets using Layer 3/Layer 4 information (for example, destination IP, DSCP value, TCP SYN/ACK, etc.).
- Queue allocation:
  - → Allocatable queues: 33 — 2000
  - → Queues 1 — 8 are default queues. They cannot be modified or deleted.
  - → Queues 9 — 32 are reserved for future use.
  - → Queues 2001 — 8000 are used for per-peer queuing.
- Specifying PIR, CIR, CBS, and MBS for the queues
- The queuing scheduler works in such a way that the queues within their CIR will be scheduled first in a round-robin fashion, followed by the queues above their CIR.
- Unclassified traffic is directed to default queues (1 — 8).

TTL Security for BGP and LDP

The BGP TTL Security Hack (BTSH) was originally designed to protect the BGP infrastructure from CPU utilization-based attacks. It is derived on the fact that the vast majority of ISP eBGP peerings are established between adjacent routers. Since TTL spoofing cannot be performed, a mechanism based on an expected TTL value can provide a simple and reasonably robust defense from infrastructure attacks based on forged BGP packets.

While TSH is most effective in protecting directly connected peers, it can also provide a lower level of protection to multi-hop sessions. When a multi-hop BGP session is required, the expected TTL value can be set to 255 minus the configured range-of-hops. This approach can provide a qualitatively lower degree of security for BGP (for example, a DoS attack could, theoretically, be launched by compromising a box in the path). However, BTSH will catch a vast majority of observed distributed DoS (DDoS) attacks against eBGP. For further information, refer to draft-gill-btsh-xx.txt, *The BGP TTL Security Hack (BTSH).*

TSH can be used to protect LDP peering sessions as well. For details, see draft-chen-ldp-ttl-xx.txt, *TTL-Based Security Option for LDP Hello Message*.

The TSH implementation supports the ability to configure TTL security per BGP/LDP peer and evaluate (in hardware) the incoming TTL value against the configured TTL value. If the incoming TTL value is less than the configured TTL value, the packets are discarded and a log is generated.

Exponential Login Backoff

A malicious user may attempt to gain CLI access by means of a dictionary attack using a script to automatically attempt to login as an “admin” user and using a dictionary list to test all possible passwords.Using the exponential-backoff feature in the **config>system>login-control** context the 7750 SR OS increases the delay between login attempts exponentially to mitigate attacks.

A malicious user may attempt to gain CLI access by means of a dictionary attack using a script to automatically attempt to login as an “admin” user and using a dictionary list to test all possible passwords.Using the exponential-backoff feature in the config>system>login-control context the 7750 SR OS increases the delay between login attempts exponentially to mitigate attacks.

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

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

The 7750 SR OS terminates after four unsuccessful tries. A wait period will never be longer than 4 seconds. The periods are fixed and will restart in subsequent sessions.

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

For example:

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

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

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

Refer to Configuring Login Controls on page 87. The commands are described in Login, Telnet, SSH and FTP Commands on page 116.

User Lockout

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

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

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

Encryption

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

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

802.1x Network Access Control

The Alcatel-Lucent 7750 SR OS supports network access control of client devices (PCs, STBs, etc.) on an Ethernet network using the IEEE. 802.1x standard. 802.1x is known as Extensible Authentication Protocol (EAP) over a LAN network or EAPOL.

TCP Enhanced Authentication Option

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

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

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

Packet Formats

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

Option Syntax

- Kind: 8 bits

  The Kind field identifies the TCP Enhanced Authentication Option. This value will be assigned by IANA.
- Length: 8 bits

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

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

  For all algorithms specified in this memo the value will be 16 octets.
- T-Bit: 1 bit

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

  The default value is 0.
- K-Bit: 1 bit

  This bit is reserved for future enhancement. Its value MUST be equal to zero.
- Alg ID: 6 bits

  The Alg ID field identifies the MAC algorithm.
- Res: 2 bits

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

  Key ID: 6 bits

  The Key ID field identifies the key that was used to generate the message digest.
- Authentication Data: Variable length
- The Authentication Data field contains data that is used to authenticate the TCP segment. This data includes, but need not be restricted to, a MAC. The length and format of the Authentication Data Field can be derived from the Alg ID.
- The Authentication for TCP-based Routing and Management Protocols draft provides and overview of the TCP Enhanced Authentication Option. The details of this feature are described in draft-bonica-tcp-auth-04.txt.

Keychain

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

Table 5: Keychain Mapping

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

Configuration Notes

This section describes security configuration caveats.

General

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

Configuring Security with CLI

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

Topics in this section include:

Setting Up Security Attributes

Configuring Authentication

Refer to the following sections to configure authentication:

- Local authentication
  - → Configuring Password Management Parameters on page 68
  - → Configuring Profiles on page 71
  - → Configuring Users on page 72
- RADIUS authentication (only)

  By default, authentication is enabled locally. Perform the following tasks to configure security on each participating 7750 SR-Series router:
  - → Configuring Profiles on page 71
  - → Configuring RADIUS Authentication on page 78
  - → Configuring Users on page 72
- RADIUS authentication

  To implement only RADIUS authentication, *with* authorization, perform the following tasks on each participating 7750 SR-Series router:
  - → Configuring RADIUS Authentication on page 78
  - → Configuring RADIUS Authorization on page 79
- TACACS+ authentication

  To implement only TACACS+ authentication, perform the following tasks on each participating 7750 SR-Series router:
  - → Configuring Profiles on page 71
  - → Configuring Users on page 72
  - → Enabling TACACS+ Authentication on page 83

Configuring Authorization

Refer to the following sections to configure authorization.

- Local authorization

  For local authorization, configure these tasks on each participating 7750 SR-Series router:

  → Configuring Profiles on page 71

  → Configuring Users on page 72

- RADIUS authorization (only)

  For RADIUS authorization (without authentication), configure these tasks on each participating 7750 SR-Series router:

  → Configuring RADIUS Authorization on page 79

  → Configuring Profiles on page 71

  For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 38.

- RADIUS authorization

  For RADIUS authorization (with authentication), configure these tasks on each participating 7750 SR-Series router:

  → Configuring RADIUS Authorization on page 79

  For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 38.

  → Configuring RADIUS Authentication on page 78

  → Configuring Profiles on page 71

- TACACS+ authorization (only)

  For TACACS+ authorization (without authentication), configure these tasks on each participating 7750 SR-Series router:

  → Configuring TACACS+ Authorization on page 84

- TACACS+ authorization

For TACACS+ authorization (with authentication), configure these tasks on each participating 7750 SR-Series router:

→ Enabling TACACS+ Authentication on page 83

→ Configuring TACACS+ Authorization on page 84

Configuring Accounting

Refer to the following sections to configure accounting.

- Local accounting is not implemented. For information about configuring accounting policies, refer to Configuring Logging with CLI on page 339
- Configuring RADIUS Accounting on page 80
- Configuring TACACS+ Accounting on page 85

Security Configurations

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

To implement security features, configure the following components:

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

The following example displays default values for security parameters.

```
A:ALA-1>config>system>security# info detail
----------------------------------------------
     no hash-control
     telnet-server
     no telnet6-server
     no ftp-server
     management-access-filter
          ip-filter
               no shutdown
          exit
          mac-filter
               no shutdown
          exit
     exit
     profile "default"
          default-action none
          no li
          entry 10
               no description
               match “exec”
               action permit
...
     password
          authentication-order radius tacplus local
          no aging
          minimum-length 6
          attempts 3 time 5 lockout 10
          complexity
     exit
     user "admin"
          password "./3kQWERTYn0Q6w" hash
          access console
     no home-directory
     no restricted-to-home
```

```
          console
               no login-exec
               no cannot-change-password
               no new-password-at-login
               member "administrative"
          exit
     exit
     snmp
          view iso subtree 1
               mask ff type included
          exit
...
          access group snmp-ro security-model snmpv1 security-level no-auth-no-privacy read 
no-security notify no-security
          access group snmp-ro security-model snmpv2c security-level no-auth-no-privacy 
read no-security notify no-security
          access group snmp-rw security-model snmpv1 security-level no-auth-no-privacy read 
no-security write no-security notify no-security
          access group snmp-rw security-model snmpv2c security-level no-auth-no-privacy 
read no-security write no-security notify no-security
          access group snmp-rwa security-model snmpv1 security-level no-auth-no-privacy 
read iso write iso notify iso
          access group snmp-rwa security-model snmpv2c security-level no auth-no-privacy 
read iso write iso notify iso
          access group snmp-trap security-model snmpv1 security-level no-auth-no-privacy 
notify iso
          access group snmp-trap security-model snmpv2c security-level no-auth-no-privacy 
notify iso
          access group cli-readonly security-model snmpv2c security-level 
no-auth-no-privacy read iso notify iso
          access group cli-readwrite security-model snmpv2c security-level 
no-auth-no-privacy read iso write iso notify iso
          attempts 20 time 5 lockout 10
     exit
     no ssh
```

Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure security and provides the CLI commands. Table 6 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 6: Security Configuration Requirements

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

Security Configuration Procedures

Configuring Management Access Filters

Creating and implementing management access filters is optional. Management access filters control all traffic going in to the CPM, including all routing protocols. They apply to packets from all ports. The filters can be used to restrict management of the 7750 SR OS router by other nodes outside either specific (sub)networks or through designated ports. By default, there are no filters associated with security options. The management access filter and entries must be explicitly created on each router. These filters also apply to the management Ethernet port.

The 7750 SR OS implementation exits the filter when the first match is found and execute the actions according to the specified action. For this reason, entries must be sequenced correctly from most to least explicit. When both **mac-filter** and **ip-filter/ipv6-filter** are to be applied to a given traffic, **mac-filter** is applied first.

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

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

CLI Syntax:
```
config>system
 security
 management-access-filter
    [no] ip-filter
    default-action {permit|deny|deny-host-unreachable}
```

```
renum old-entry-number new-entry-number
   [no] shutdown
   [no] entry entry-id
      [no] action {permit|deny|deny-host-unreachable}
      [no] description <description-string>
      [no] dst-port port [mask]
      [no] log
      [no] protocol protocol-id
      [no] router router-instance | service-id | service-
      name service-name
      [no] src-ip {ip-prefix/mask |ip-prefix netmask}
      [no] src-port{port-id|cpm|lag lag-id}
ipv6-filter
default-action {permit|deny|deny-host-unreachable}
renum old-entry-number new-entry-number
   [no] shutdown
   [no] entry entry-id
      [no] action {permit|deny|deny-host-unreachable}
      [no] description description-string
      [no] dst-port port [mask]
      [no] flow-labelvalue
      [no] log
      [no] next-header next-header
      [no] router router-name|service-id | service-name
      service-name
      [no] src-ip pv6-address/prefix-length
      [no] src-port {port-id|cpm|lag lag-id}
mac-filter
   default-action {permit|deny}
   renum old-entry-number new-entry-number
      [no] shutdown
      [no] entry entry-id
         [no] action deny | permit
         [no] description description-string
         [no] log
         [no] match [frame-type frame-type]
            [no] cfm-opcode {lt|gt|eq} pcode | range start
            end>
            [no] dot1p dot1p-value [dot1p-mask]
            [no] dsap dsap-value [dsap-mask]
            [no] dst-mac ieee-address [ieee-address-mask]
            [no] etype 0x0600..0xffff
            [no] snap-oui {zero|non-zero}
            [no] snap-pid snap-pid
            [no] src-mac ieee-address [ieee-address-mask]
            [no] ssap ssap-value [ssap-mask]
            [no] svc-id <ervice-id
```

The following displays a management access filter configuration example:

```
*A:Dut-C>config>system>security>mgmt-access-filter# info
----------------------------------------------
                ip-filter
                    default-action deny
                    entry 10
                        description "Accept SSH from mgmnt subnet"
                        src-ip 192.168.5.0/26
                        protocol tcp
                        dst-port 22 65535
                        action permit
                    exit
                exit
                ipv6-filter
                    default-action permit
                    entry 10
                        src-ip 3FFE::1:1/128
                        next-header rsvp
                        log
                        action deny
                    exit
                exit
                mac-filter
                    default-action permit
                    entry 12
                        match frame-type ethernet_II
                            svc-id 1
                            src-mac 00:01:01:01:01:01 ff:ff:ff:ff:ff:ff
                        exit
                        action permit
                    exit
                exit
----------------------------------------------
*A:Dut-C>config>system>security>mgmt-access-filter#
```

Configuring IP CPM Filters

CPM filters and queues control all traffic going in to the CPM, 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 and queuing is performed by network processor hardware using no resources on the main CPUs.

Use the following CLI commands to configure a CPM filter.

CLI Syntax:
```
config>system>security
 cpm-filter
    default-action {accept | drop}
    ip-filter
       renum old-entry-id new-entry-id
          [no] shutdown
          [no] entry entry-id [create]
             [no] action accept | drop | queue queue-id
             [no] description description-string
             [no] log log-id
             [no] match [protocol protocol-id>
             [no] dscp dscp-name
             [no] dst-ip {ip-address/mask|ip-address net-
             mask|ip-prefix-list prefix-list-name }
             [no] dst-port tcp/udp port-number [mask]
             [no] fragment {true|false}
             [no] icmp-code icmp-code
             [no] icmp-type icmp-type
             [no] ip-option ip-option-value [ip-option-mask]
             [no] multiple-option {true|false}
             [no] option-present {true|false}
             [no] router router-name|service-id | service-
             name service-name
             [no] src-ip {ip-address/mask|ip-address net-
             mask|ip-prefix-list prefix-list-name}
             [no] src-port src-port-number [mask]
             [no] tcp-ack {true|false}
             [no] tcp-syn {true|false}
    ipv6-filter
       renum <old-entry-id> <new-entry-id>
          [no] shutdown
          [no] entry entry-id [create]
             [no] action accept | drop | queue queue-id
                     [no] description description-string
             [no] log log-id
             [no] match [next-header next-header]
                [no] dscp dscp-name
```

```
            [no] dst-ip ipv6-address/prefix-length
            [no] dst-port tcp/udp port-number [mask>
            [no] flow-label value
            [no] icmp-code icmp-code
            [no] icmp-type icmp-type
            [no] router router-name|service-id | service-
            name service-name
            [no] src-ip ipv6-address/prefix-length
            [no] src-port src-port-number [mask]
            [no] tcp-ack {true|false}
            [no] tcp-syn {true|false}
mac-filter
   renum <old-entry-id> new-entry-id
      [no] shutdown
      [no] entry <entry-id> [create]
         [no] action accept | drop | queue queue-id
         [no] description description-string
         [no] log log-id
         [no] match [frame-type frame-type]
            [no] cfm-opcode range start end | {lt|gt|eq}
            opcode
            [no] dsap dsap-value [dsap-mask]
            [no] dst-mac ieee-address [ieee-address-mask]
            [no] etype 0x0600..0xffff
            [no] src-mac ieee-address [ieee-address-mask]
            [no] ssap ssap-value [ssap-mask]
            [no] svc-id service-id
```

The following displays an IP CPM filter configuration example:

```
*A:Dut-C>config>sys>security>cpm-filter# info
----------------------------------------------
                ip-filter
                    shutdown
                    entry 100 create
                        action queue 50
                        log 110
                        match protocol icmp
                            fragment true
                            icmp-type dest-unreachable
                            icmp-code host-unreachable
                            multiple-option false
                            option-present true
                            src-ip 192.100.2.0/24
                        exit
                    exit
                exit
                ipv6-filter
                    shutdown
                    entry 30 create
                        action drop
                        log 190
                        match next-header tcp
                            dscp ef
                            dst-ip 3FFE::2:2/128
                            src-port 100 100
                            tcp-syn true
                            tcp-ack false
                            flow-label 10
                        exit
                    exit
                exit
                mac-filter
                    shutdown
                    entry 40 create
                        action accept
                        log 101
                        match frame-type ethernet_II
                            svc-id 12
                            dst-mac 00:03:03:03:01:01 ff:ff:ff:ff:ff:ff
                            etype 0x8902
                            cfm-opcode gt 100
                        exit
                    exit
                exit
----------------------------------------------
*A:Dut-C>config>sys>security>cpm-filter#
```

Configuring MAC CPM Filters

CPM filters and queues control all traffic going in to the CPM, 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 and queuing is performed by network processor hardware using no resources on the main CPUs.

The following displays a MAC CPM filter configuration example:

```
*A:ALA-49>config>sys>sec>cpm>mac-filter# info
----------------------------------------------
                    entry 10 create
                        description "MAC-CPM-Filter 10.10.10.100 #007"
                        match
                        exit
                        log 101
                        action drop
                    exit
                    entry 20 create
                        description "MAC-CPM-Filter 10.10.10.100 #008"
                        match
                        exit
                        log 101
                        action drop
                    exit
                    no shutdown
----------------------------------------------
*A:ALA-49>config>sys>sec>cpm>mac-filter#
```

Configuring IPv6 CPM Filters

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
          action {accept | drop}
          description description-string
          log log-id
          match [next-header next-header]
             dscp dscp-name
             dst-ip ipv6-address/prefix-length
             dst-port [tcp/udp port-number] [mask]
             flow-label value
             icmp-code icmp-code
             icmp-type icmp-type
             router [router-name |service-id]
             src-ip ipv6-address/prefix-length
             src-port src-port-number [mask]
             tcp-ack {true|false}
             tcp-syn {true|false}
       renum old-entry-id new-entry-id
```

The following example displays a CPM filter configuration:

```
A:ALA-48>config>sys>sec>cpm>ipv6-filter# info
----------------------------------------------
                    entry 10 create
                        description "IPv6 CPM Filter"
                        log 101
                        match next-header igp
                            dst-ip 1000:1:1:1:1:1:1:1/112
                            src-ip 2000:1::1/96
                            flow-label 5000
                        exit
                    exit
                    entry 20 create
                        description "CPM-Filter 10.4.101.2 #201"
                        log 101
                        match next-header tcp
                            dscp af11
                            dst-ip 3FEE:12E1:2AC1:EA32::/64
                            src-ip 3FEE:1FE1:2AC1:EA32::/64
                            flow-label 5050
                        exit
                    exit
                    no shutdown
----------------------------------------------
A:ALA-48>config>sys>sec>cpm>ipv6-filter#
```

Configuring CPM Queues

Use the following CLI commands to configure a CPM queue. The first queue available is 33.

CLI Syntax:

```
config>system>security# cpm-queue
 queue queue-id
    cbs cbs
    mbs mbs
    rate rate [cir cir]
```

The following example displays a CPM queue configuration:

```
A:ALA-987>config>sys>security>cpm-queue# info
----------------------------------------------
                queue 33 create
                exit
                queue 101 create
                    cbs 5
                    mbs 5
                    rate 5 cir 5
                exit
                queue 102 create
                    cbs 5
                    mbs 5
                    rate 5 cir 5
                exit
                queue 103 create
                    cbs 5
                    mbs 5
                    rate 5 cir 5
                exit
                queue 104 create
                    cbs 5
                    mbs 5
                    rate 5 cir 5
----------------------------------------------

A:ALA-987>config>sys>security>cpm-queue#
```

Configuring Password Management Parameters

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

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

Use the following CLI commands to configure password support:

CLI Syntax:

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

The following example displays a password configuration:

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

IPSec Certificates Parameters

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

```
*A:SR-7/Dut-A# admin certificate import type cert input cf3:/pre-import/R1-0cert.pem out-
put R1-0cert.der format pem
```

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

```
*A:SR-7/Dut-A#  admin certificate export type cert input R1-0cert.der output cf3:/R1-
0cert.pem format pem
```

The following displays an example of profile output:

```
*A:SR-7/Dut-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:SR-7/Dut-A>config>system>security>pki#
```

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

```
:SR-7/Dut-A>config>ipsec>ike-policy# info
----------------------------------------------
            ike-version 2
            auth-method cert-auth
            own-auth-method psk
----------------------------------------------
```

The following displays an example ofa 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 30.1.1.13 peer 50.1.1.15 delivery-service 300
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "Sanity-1"
                            transform 1
                            cert
                                trust-anchor "R1-0"
                                cert "M2cert.der"
                                key "M2key.der"
                            exit
                        exit
                        no shutdown
                    exit
                exit
            exit
```

Configuring Profiles

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

Use the following CLI commands to configure user profiles:

CLI Syntax:

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

The following example displays a user profile output:

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

Configuring Users

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

CLI Syntax:

```
config>system>security
 user user-name
    access [ftp] [snmp] [console] [li]
    console
       cannot-change-password
       login-exec url-prefix:source-url
       member user-profile-name [user-profile-name...(up to 8
          max)]
       new-password-at-login
    home-directory url-prefix [directory][directory/directory
       ..]
    password [password] [hash|hash2]
    restricted-to-home
    snmp
       authentication {[none]|[[hash] {md5 key-1|sha key-1}
          privacy {none|des-key|aes-128-cfb-key key-2]}
       group group-name
 user-template template-name
```

The following displays a user configuration example:

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

Configuring Keychains

The following displays a keychain configuration.

```
A:ALA-1>config>system>security# info
----------------------------------------------
...
            keychain "abc"
                direction
                    bi
                        entry 1 key "ZcvSElJzJx/wBZ9biCtOVQJ9YZQvVU.S" hash2 alg
orithm aes-128-cmac-96
                            begin-time 2006/12/18 22:55:20
                        exit
                    exit
                exit
            exit
            keychain "basasd"
                direction
                    uni
                        receive
                            entry 1 key "Ee7xdKlYO2DOm7v3IJv/84LIu96R2fZh" hash2
 algorithm aes-128-cmac-96
                                tolerance forever
                            exit
                        exit
                    exit
                exit
            exit
...
----------------------------------------------
A:ALA-1>config>system>security#
```

Copying and Overwriting Users and Profiles

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

User

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

Example:

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

The following output displays the copied user configurations:

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

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

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

Profile

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

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

The following output displays the copied profiles:

```
A:ALA-49>config>system>security# info
----------------------------------------------
...
A:ALA-49>config>system>security# info detail
----------------------------------------------
...
            profile "default"
                default-action none
                entry 10
                    no description
                    match "exec"
                    action permit
                exit
                entry 20
                    no description
                    match "exit"
                    action permit
                exit
                entry 30
                    no description
                    match "help"
                    action permit
                exit
                entry 40
                    no description
                    match "logout"
                    action permit
                exit
                entry 50
                    no description
                    match "password"
                    action permit
                exit
                entry 60
                    no description
                    match "show config"
                    action deny
                exit
                entry 70
                    no description
                    match "show"
                    action permit
                exit
                entry 80
                    no description
                    match "enable-admin"
                    action permit
                exit
            exit
            profile "testuser"
                default-action none
                entry 10
                    no description
                    match "exec"
                    action permit
                exit
                entry 20
                    no description
                    match "exit"
                    action permit
                exit
                entry 30
                    no description
                    match "help"
                    action permit
                exit
                entry 40
                    no description
                    match "logout"
                    action permit
                exit
                entry 50
                    no description
                    match "password"
                    action permit
                exit
                entry 60
                    no description
                    match "show config"
                    action deny
                exit
                entry 70
                    no description
                    match "show"
                    action permit
                exit
                entry 80
                    no description
                    match "enable-admin"
                    action permit
                exit
            exit
            profile "administrative"
                default-action permit-all exit
...
----------------------------------------------
A:ALA-12>config>system>security#
```

RADIUS Configurations

Configuring RADIUS Authentication

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

Also, the system IP address must be configured in order for the RADIUS client to work. See Configuring a System Interface of the 7750 SR OS Router Configuration Guide.

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

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

CLI Syntax:

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

The following displays a RADIUS authentication configuration example:

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

Configuring RADIUS Authorization

In order for RADIUS authorization to function, RADIUS authentication *must* be enabled first. See Configuring RADIUS Authentication on page 78.

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 38.

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

CLI Syntax:

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

The following displays a RADIUS authorization configuration example:

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

Configuring RADIUS Accounting

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

CLI Syntax:

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

The following displays RADIUS accounting configuration example:

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

Configuring 802.1x RADIUS Policies

Use the following CLI commands to configure generic authentication parameters for clients using 802.1x EAPOL. Additional parameters are configured per Ethernet port. Refer to the 7750 SR OS Interface Configuration Guide

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

CLI Syntax:

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

The following displays a 802.1x configuration example:

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

Configuring CPU Protection Policies

The CPU protection features are supported on the 7750 SR-7/12 platforms.   These features are not available on the 7750 SR-1 or 7750 SR-c12.

The following output displays a configuration of the CPU protection parameters and a CPU protection policy:

```
Node_3>config>sys>security>cpu-protection# info
----------------------------------------------
                link-specific-rate 4000
                policy 4 create
                    no alarm
                    description "My new CPU Protection policy"
                    overall-rate 9000
                    per-source-rate 2000
                    out-profile-rate 4000
                exit
                policy 254 create
                exit
                policy 255 create
                exit
                port-overall-rate 12000
                protocol-protection
----------------------------------------------
Node_3>config>sys>security>cpu-protection#
```

The following output displays an application to an interface:

```
Node_3>config>service>ies>if# info
----------------------------------------------
                cpu-protection 4
                sap 1/1/5 create
                exit
----------------------------------------------
Node_3>config>sys>security>cpu-protection#
```

TACACS+ Configurations

Enabling TACACS+ Authentication

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

Use the following CLI commands to configure profiles:

CLI Syntax:

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

The following displays a TACACS+ authentication configuration example:

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

Configuring TACACS+ Authorization

In order for TACACS+ authorization to function, TACACS+ authentication *must* be enabled first. See Enabling TACACS+ Authentication on page 83.

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

CLI Syntax:

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

The following displays a TACACS+ authorization configuration example:

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

Configuring TACACS+ Accounting

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

CLI Syntax:

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

The following displays a TACACS+ accounting configuration example:

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

Enabling SSH

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

CLI Syntax:

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

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

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

Configuring Login Controls

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

To configure login controls, enter the following CLI syntax.

CLI Syntax:

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

The following displays a login control configuration example:

```
A:ALA-1>config>system# info
----------------------------------------------
...
       login-control
           ftp
               inbound-max-sessions 5
           exit
           telnet
               inbound-max-sessions 7
               outbound-max-sessions 2
           exit
           idle-timeout 1440
           pre-login-message "Property of Service Routing Inc. Unauthorized access prohib-
ited."
           motd text "Notice to all users: Software upgrade scheduled 3/2 1:00 AM"
       exit
      no exponential-backoff
...
----------------------------------------------
A:ALA-1>config>system#
```

Security Command Reference

Command Hierarchies

Configuration Commands

Security Commands

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

LLDP Commands

```
configure
    — system
        — lldp
            — message-fast-tx time
            — no message-fast-tx
            — message-fast-tx-init count
            — no message-fast-tx-init
            — notification-interval time
            — no notification-interval
            — reinit-delay time
            — no reinit-delay
            — tx-credit-max count
            — no tx-credit-max
            — tx-hold-multiplier multiplier
            — no tx-hold-multiplier
            — tx-interval interval
            — no tx-interval
```

CPM Filter Commands

```
config
    — system
        — security
            — [no] cpm-filter
                — default-action {accept | drop}
```

IP CPM Filter Commands

```
config
    — system
        — security
            — [no] cpm-filter
                — [no] ip-filter
                    — [no] entry entry-id
                        — action [accept | drop | queue queue-id]}
                        — 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 netmask}
                            — 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
                            — router service-name service-name
                            — router [router-instance]
                            — no router
                            — src-ip {ip-address/mask | ip-address netmask}
                            — no src-ip
                            — src-port [src-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
```

IPv6 CPM Filter Commands

```
config
     — system
          — security
               — [no] cpm-filter
                    — [no] ipv6-filter
                         — [no] entry entry-id
                              — action [accept | drop | queue queue-id]}
                              — 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]
                                 — no dst-ip
                                 — dst-port [tcp/udp port-number] [mask]
                                 — no dst-port
                                 — flow-label value
                                 — no flow-label
                                 — icmp-code icmp-code
                                 — no icmp-code
                                 — icmp-type icmp-type
                                 — no icmp-type
                                 — router [router-name | service-id]
                                 — no router
                                 — src-ip [ipv6-address/prefix-length]
                                 — no src-ip
                                 — src-port [src-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
```

MAC CPM Filter Commands

```
config
     — system
          — security
               — [no] cpm-filter
                    — [no] mac-filter
                         — [no] entry entry-id
                              — action [accept | drop | queue queue-id]}
                              — no action
                              — description description-string
                              — no description
                              — log log-id
                              — no log
                              — match [frame-type frame-type]
                              — no match
                                   — cfm-opcode {lt | gt | eq} opcode
                                   — cfm-opcode range start end
                                   — no cfm-opcode
                                   — dsap dsap-value [dsap-mask]
                                   — dst-mac ieee-address [ieee-address-mask]
                                   — no dst-mac
                                   — etype 0x0600..0xfff
                                   — no etype
                                   — src-mac ieee-address [ieee-address-mask]
                                   — no src-mac
                                   — ssap ssap-value [ssap-mask]
                                   — no ssap
                                   — svc-id service-id
                                   — no svc-id
                         — renum old-entry-number new-entry-number
                         — [no] shutdown
```

CPM Queue Commands

```
config
    — system
            — security
                    — [no] cpm-queue
                            — [no] queue queue-id
                                    — cbs cbs
                                    — no cbs
                                    — mbs mbs
                                    — no mbs
                                    — rate rate [cir cir]
                                    — no rate
```

CPU Protection Commands

```
config
    — system
        — security
            — cpu-protection
                — link-specific-rate packet-rate-limit
                — no link-specific-rate
                — policy cpu-protection-policy-id [create]
                — no policy cpu-protection-policy-id
                    — [no] alarm
                    — description description-string
                    — no description
                    — eth-cfm entry <entry> levels <levels> opcodes <opcodes> rate
                      <packet-rate-limit>
                    — no eth-cfm
                    — out-profile-rate packet-rate-limit
                    — no out-profile-rate
                    — overall-rate packet-rate-limit
                    — no overall-rate
                    — per-source-rate packet-rate-limit
                    — no per-source-rate
                — port-overall-rate packet-rate-limit
                — no port-overall-rate
                — [no] protocol-protection [allow-sham-links]
```

Refer to the OS Services Guide and the Multi-Service ISA Guide for command, syntax, and usage information about applying CPU Protection policies to interfaces.

CPU protection policies are applied by default (and customer policies can be applied) to a variety of entities including interfaces and SAPs. Refer to the appropriate guides (See Preface for document titles) for command syntax and usage for applying CPU protection policies. Examples of entities that can have CPU protection policies applied to them include:

configure>router>interface>cpu-protection *policy-id*

configure>service>epipe>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>epipe>spoke-sdp>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>ies>interface>cpu-protection *policy-id*

configure>service>ies>interfac>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>template>vpls-sap-template>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vpls>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vpls>video-interface>cpu-protection *policy-id*

configure>service>vprn>interface>cpu-protection *policy-id*

configure>service>vprn >interface>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vprn>network-interface>cpu-protection *policy-id*

configure>service>vprn>subscriber-interface>group-interface>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>subscriber-mgmt>msap-policy>cpu-protection *policy-id* [**mac-monitoring**]

Management Access Filter Commands

```
config
    — system
        — security
            — [no] management-access-filter
                — [no] ip-filter
                    — default-action {permit | deny}
                    — [no] entry entry-id
                        — action {permit | deny | deny-host-unreachable}
                        — no action
                        — description description-string
                        — no description
                        — dst-port value [mask]
                        — no dst-port
                        — protocol  protocol-id
                        — no protocol
                        — router {router-instance}
                        — no router
                        — src-ip {ip-prefix/mask | ip-prefix netmask}
                        — no src-ip
                        — src-port {port-id | cpm | lag lag-id }
                        — no src-port
                        — src-port old-entry-number new-entry-number
                    — renum old-entry-number new-entry-number
                    — [no] shutdown
                — [no] ipv6-filter
                    — default-action {permit | deny | deny-host-unreachable}
                    — [no] entry entry-id
                        — action {permit | deny | deny-host-unreachable}
                        — no action
                        — description description-string
                        — no description
                        — dst-port value [mask]
                        — no dst-port
                        — flow-label value
                        — no flow-label
                        — [no] log
                        — next-header next-header
                        — no next-header
                        — router {router-instance}
                        — no router
                        — src-ip {ip-prefix/mask | ip-prefix netmask}
                        — no src-ip
                        — src-port {port-id | cpm | lag lag-id }
                        — no src-port
                    — renum old-entry-number new-entry-number
                    — [no] shutdown
                — [no] mac-filter
                    — default-action {permit | deny}
                    — [no] entry entry-id
                        — action {permit | deny | deny-host-unreachable}
                        — no action
                        — description description-string
                        — no description
                        — [no] log
                        — match frame-type frame-type
                        — no match
                            — cfm-opcode {lt | gt | eq} opcode
                            — cfm-opcode range start end
                            — no cfm-opcode
                            — dot1p dot1p-value [dot1p-mask]
                            — dsap dsap-value [dsap-mask]
                            — dst-mac ieee-address [ieee-address-mask]
                            — no dst-mac
                            — etype 0x0600..0xfff
                            — no etype
                            — snap-oui {zero | non-zero}
                            — snap-pid snap-pid
                            — no snap-pid
                            — src-mac ieee-address [ieee-address-mask]
                            — no src-mac
                            — ssap ssap-value [ssap-mask]
                            — no ssap
                            — svc-id service-id
                            — no svc-id
                    — renum old-entry-number new-entry-number
                    — [no] shutdown
```

Security Password Commands

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

Public Key Infrastructure (PKI) Commands

```
config
    — system
        — security
            — pki
                — ca-profile name [create]
                — no ca-profile name
                    — cert-file filename
                    — no cert-file
                    — crl-file filename
                    — no crl-file
                    — description description-string
                    — no description
                    — [no] shutdown
                — maximum-cert-chain-depth level
                — no maximum-cert-chain-depth
admin
    — http-download http-url to local-url router {base|management} [force]
    — certificate
        — display type {cert|key|crl|cert-request} url-string format {pkcs10|pkcs12|pkcs7-der|pkcs7-
          pem|pem|der} [password [32 chars max]]
        — export type {cert|key|crl} input filename output url-string format output-format [password [32
          chars max]] [pkey filename]
        — gen-keypair url-string [size {512|1024|2048}] [type {rsa|dsa}]
        — gen-local-cert-req keypair url-string subject-dn subject-dn [domain-name [255 chars max]] [ip-
          addr ip-address] file url-string
        — import type {cert|key|crl} input url-string output filename format input-format [password [32
          chars max]]
        — reload type {cert|key} filename
```

Profile Commands

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

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
                    — [no] use-default-template
```

SSH Commands

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

TACPLUS Commands

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

User Commands

```
config
     — system
          — security
               — [no] user user-name
```

```
                    — [no] access [ftp] [snmp] [console] [li]
                    — console
                         — [no] cannot-change-password
                         — login-exec url-prefix::source-url
                         — no login-exec
                         — member user-profile-name [user-profile-name…(up to 8 max)]
                         — no member user-profile-name
                         — [no] new-password-at-login
                    — home-directory url-prefix [directory] [directory/directory…]
                    — no home-directory
                    — password [password] [hash | hash2]
                    — [no] restricted-to-home
                    — snmp
                         — authentication {[none] | [[hash] {md5 key-1 | sha key-1 } privacy
                           {none|des-key|aes-128-cfb-key key-2}]}
                         — group group-name
                         — no group
```

User Template Commands

```
config
     — system
          — security
               — user-template {tacplus_default | radius_default}
                    — [no] access [ftp] [console]
                    — console
                         — login-exec url-prefix:source-url
                         — no login-exec
                    — home-directory url-prefix [directory][directory/directory..]
                    — no home-directory
                    — profile user-profile-name
                    — no profile
                    — [no] restricted-to-home
```

Dot1x Commands

```
config
     — system
          — security
               — dot1x
                    — radius-plcy name
                         — retry count
                         — no retry
                         — server (dot1x) server-index address ip-address secret key [port port]
                         —  source-address ip-address
                         — [no] shutdown
                         — timeout seconds
                         — no timeout
                    — [no] shutdown
```

Keychain Commands

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

TTL Security Commands

```
config
     — router
               — bgp
                         — group
                                   — ttl-security min-ttl-value
                                   — neighbor
                                             — ttl-security min-ttl-value
config
     — router
               — ldp
                         — peer-parameters
                                   — peer
                                             — ttl-security min-ttl-value
config
     — system
               — login-control
                         — ssh
                                   — ttl-security
config
     — system
               — login-control
                         — telnet
```

```
                                                  — ttl-security
```

Login Control Commands

```
config
    — system
            — login-control
                    — [no] exponential-backoff
                    — ftp
                            — inbound-max-sessions value
                            — no inbound-max-sessions
                    — idle-timeout {minutes | disable}
                    — no idle-timeout
                    — [no] login-banner
                    — motd {url url-prefix: source-url | text motd-text-string}
                    — no motd
                    — pre-login-message login-text-string [name]
                    — no pre-login-message
                    — ssh
                            — disable-graceful-shutdown
                            — inbound-max-sessions
                            — outbound-max-sessions
                            — ttl-security
                    — telnet
                            — enable-graceful-shutdown
                            — inbound-max-sessions value
                            — no inbound-max-sessions
                            — outbound-max-sessions value
                            — no outbound-max-sessions
                            — ttl-security
```

Show Commands

Security

```
show
    — system
        — security
            — access-group [group-name]
            — authentication [statistics]
            — communities
            — cpm-filter
                — ip-filter [entry entry-id]
                — ipv6-filter [entry entry-id]
            — cpm-queue queue-id
            — cpu-protection
                — excessive-sources [service-id service-id sap-id sap-id]
                — policy [policy-id] association
                — protocol-protection
                — violators [port] [interface] [sap] [video]
            — keychain keychain-name [detail]
            — management-access-filter
                — ip-filter [entry entry-id]
                — ipv6-filter  [entry entry-id]
                — mac-filter [entry entry-id]
            — password-options
            — per-peer-queuing
            — profile [profile-name]
            — source-address
            — ssh
            — user [user-id] [detail]
            — view [view-name] [detail]
```

Login Control

```
show
    — user
```

Clear Commands

Authentication

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

CPM Filter

```
    — cpm-filter
            — ip-filter [entry entry-id]
            — ipv6-filter [entry entry-id]
            — mac-filter [entry entry-id]
```

CPU Protection

```
clear
    — cpu-protection
            — excessive-sources
            — protocol-protection
            — violators [port] [interface] [sap]
```

Clear CPU Stats

```
clear
    — cpm-queue queue-id
```

Clear RADIUS Proxy Server

```
clear
    — router
            — radius-proxy-server server-name statistics
```

Debug Commands

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

Configuration Commands

General Security Commands

description

Syntax **description** *description-string*
no description

Context config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>mgmt-access-filter>ipv6-filter>entry
config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry
config>sys>sec>cpm>mac-filter>entry
config>sys>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry
config>system>security>pki>ca-profile
config>sys>security>cpu-protection>policy
config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry

Description This command creates a text description stored in the configuration file for a configuration context. This command associates a text string with a configuration context to help identify the context in the configuration file.

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

Default No description associated with the configuration context.

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

shutdown

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

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-access-filter>ipv6-filter
config>sys>sec>cpm>ip-filter
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>pki>ca-profile

config>sys>sec>cpm>ipv6-filter
config>sys>sec>cpm>mac-filter>entry

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of the command puts an entity into the administratively enabled state.

Default no shutdown

security

Syntax **security**

Context config>system

Description This command creates the context to configure security settings.

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

ftp-server

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

Context config>system>security

Description This command enables FTP servers running on the system.

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

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

hash-control

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

Context config>system>security

Description Whenever the user executes a **save** or **info** command, the system will encrypt all passwords, MD5 keys, etc., for security reasons. At present, two algorithms exist.

The first algorithm is a simple, short key that can be copied and pasted in a different location when the user wants to configure the same password. However, because it is the same password and the hash key is limited to the password/key, even the casual observer will notice that it is the same key.

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

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

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

write-version {**1** | **2**} **—** Select the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.

per-peer-queuing

Syntax [**no**] **per-peer-queuing**

Context config>system>security

Description This command enables CPM hardware queuing per peer. This means that when a peering session is established, the router will automatically allocate a separate CPM hardware queue for that peer.

The **no** form of the command disables CPM hardware queuing per peer.

Default per-peer-queuing

source-address

Syntax **source-address**

Context config>system>security

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

This feature only applies on inband interfaces and does not apply on the outband management interface. Packets going out the management interface will keep using that as source IP address. IN other words, when the RADIUS server is reachable through both the management interface and a network interface, the management interface is used despite whatever is configured under the source-address statement.

application

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

Context config>system>security>source-address

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

Parameters *app* — Specify the application name.

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

ip-int-name | *ip-address* — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

application6

Syntax **application6** *app ipv6-address*
no application6

Context config>system>security>source-address

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

Parameters *app* — Specify the application name.

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

ipv6-address — Specifies the name of the IPv6 address.

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 7750 SR networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries.

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

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 server are enabled.

The **no** form of the command disables Telnet IPv6 servers running on the system.

vprn-network-exceptions

Syntax **vprn-network-exceptions** *number seconds*

Context config>system>security

Description This command configures the rate to limit for replies to all TTL expiry and ICMP messages received within all VPRN sentences in the system and from all network IP interfaces.

The **no** form of the command disables the rate limiting of the reply to these packets.

Default no security vprn-network-exceptions

Parameters *number* — 10 — 10,000

seconds — 1 — 60

LLDP Commands

lldp

Syntax **lldp**

Context config>system

Description This command enables the context to configure system-wide Link Layer Discovery Protocol parameters.

message-fast-tx

Syntax **message-fast-tx** *time*
no message-fast-tx

Context config>system>lldp

Description This command configures the duration of the fast transmission period.

Parameters *time* — Specifies the fast transmission period in seconds.

Values 1 — 3600

Default 1

message-fast-tx-init

Syntax **message-fast-tx-init** *count*
no message-fast-tx-init

Context config>system>lldp

Description This command configures the number of LLDPDUs to send during the fast transmission period.

Parameters *count* — Specifies the number of LLDPDUs to send during the fast transmission period.

Values 1 — 8

Default 4

notification-interval

Syntax **notification-interval** *time*
no notification-interval

Context config>system>lldp

Description This command configures the minimum time between change notifications.

Parameters *time* — Specifies the minimum time, in seconds, between change notifications.

Values 5 — 3600

Default 5

reinit-delay

Syntax **reinit-delay** *time*
no reinit-delay

Context config>system>lldp

Description This command configures the time before re-initializing LLDP on a port.

Parameters *time* — Specifies the time, in seconds, before re-initializing LLDP on a port.

Values 1 — 10

Default 2

tx-credit-max

Syntax **tx-credit-max** *count*
no tx-credit-max

Context config>system>lldp

Description This command configures the maximum consecutive LLDPDUs transmitted.

Parameters *count* — Specifies the maximum consecutive LLDPDUs transmitted.

Values 1 — 100

Default 5

tx-hold-multiplier

Syntax **tx-hold-multiplier** *multiplier*
no tx-hold-multiplier

Context config>system>lldp

Description This command configures the multiplier of the tx-interval.

Parameters *multiplier* — Specifies the multiplier of the tx-interval.

Values 2 — 10

Default 4

tx-interval

Syntax **tx-interval** *interval*
no tx-interval

Context config>system>lldp

Description This command configures the LLDP transmit interval time.

Parameters *interval* — Specifies the LLDP transmit interval time.

Values 1 — 100

Default 5

Login, Telnet, SSH and FTP Commands

exponential-backoff

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

Context config>system>login-control

Description This command enables the exponential-backoff of the login prompt. The exponential-backoff command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try **admin** with any conceivable password.

The **no** form of the command disables exponential-backoff.

Default no exponential-backoff

ftp

Syntax **ftp**

Context config>system>login-control

Description This command creates the context to configure FTP login control parameters.

idle-timeout

Syntax **idle-timeout** {*minutes* | **disable**}
no idle-timeout

Context config>system>login-control

Description This command configures the idle timeout for FTP, console, or Telnet sessions before the session is terminated by the system.

By default, an idle FTP, console, SSH or Telnet session times out after 30 minutes of inactivity. This timer can be set per session.

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

Default **30** — Idle timeout set for 30 minutes.

Parameters *minutes* — The idle timeout in minutes. Allowed values are 1 to 1440. 0 implies the sessions never timeout.

Values 1 — 1440

disable — When the **disable** option is specified, a session will never timeout. To re-enable idle timeout, enter the command without the disable option.

inbound-max-sessions

Syntax **inbound-max-sessions** *value*
no inbound-max-sessions

Context config>system>login-control>ftp

Description This command configures the maximum number of concurrent inbound FTP sessions.

This value is the combined total of inbound and outbound sessions.

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

Default 3

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

Values 0 — 5

inbound-max-sessions

Syntax **inbound-max-sessions** *value*
no inbound-max-sessions

Context config>system>login-control>telnet

Description This parameter limits the number of inbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established to the router. The local serial port cannot be disabled.

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

Default 5

Parameters *value* — The maximum number of concurrent inbound Telnet sessions, expressed as an integer.

Values 0 — 15

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 7750 SR OS copyright and build date information for a console login attempt.

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

login-control

Syntax **login-control**

Context config>system

Description This command creates the context to configure the session control for console, Telnet and FTP.

motd

Syntax **motd** {**url** *url-prefix*: *source-url* | **text** *motd-text-string*}
no motd

Context config>system>login-control

Description This command creates the message of the day displayed after a successful console login. Only one message can be configured.

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

Default No **motd** is defined.

Parameters **url** *url-prefix*: *source-url* — When the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote.

text *motd-text-string* — The text of the message of the day. The *motd-text-string* must be enclosed in double quotes. Multiple text strings are not appended to one another.

Some special characters can be used to format the message text. The "\n" character creates multi-line MOTDs and the "\r" character restarts at the beginning of the new line. For example, entering "\n\r" will start the string at the beginning of the new line, while entering "\n" will start the second line below the last character from the first line.

outbound-max-sessions

Syntax **outbound-max-sessions** *value*
no outbound-max-sessions

Context config>system>login-control>telnet

Description This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled.

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

Default 5

Parameters *value* — The maximum number of concurrent outbound Telnet sessions, expressed as an integer.

Values 0 — 15

pre-login-message

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

Context config>system>login-control

Description This command creates a message displayed prior to console login attempts on the console via Telnet.

Only one message can be configured. If multiple **pre-login-messages** are configured, the last message entered overwrites the previous entry.

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

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

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

Parameters *login-text-string* — The string can be up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

name — When the keyword *name* is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.

ssh

Syntax **ssh**

Context config>system>login-control

Description This command enables the context to configure the SSH parameters.

disable-graceful-shutdown

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

Context config>system>login-control>ssh

Description This command enables graceful shutdown of SSH sessions.

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

preserve-key

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

Context config>system>security>ssh

Description After enabling this command, private keys, public keys, and host key file will be saved by the server. It is restored following a system reboot or the ssh server restart.

The **no** form of the command specifies that the keys will be held in memory by the SSH server and is not restored following a system reboot.

Default no preserve-key

server-shutdown

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

Context config>system>security>ssh

Description This command enables the SSH servers running on the system.

Default At system startup, only the SSH server is enabled.

version

Syntax **version** *ssh-version*
no version

Context config>system>security>ssh

Description Specifies the SSH protocol version that will be supported by the SSH server.

Default 2

Parameters *ssh-version* — Specifies the SSH version.

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

telnet

Syntax **telnet**

Context config>system>login-control

Description This command creates the context to configure the Telnet login control parameters.

enable-graceful-shutdown

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

Context config>system>login-control>telnet

Description This command enables graceful shutdown of telnet sessions.

The no form of the command disables graceful shutdown of telnet sessions.

Management Access Filter Commands

management-access-filter

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

Context config>system>security

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

Management access filters control all traffic in and out of the CPM. They can be used to restrict management of the 7750 SR-Series router by other nodes outside either specific (sub)networks or through designated ports.

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

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

Default No management access filters are defined.

ip-filter

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

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

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

ipv6-filter

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

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

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

action

Syntax **action** {**permit | deny | deny-host-unreachable**}
no action

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

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

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

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

Default none — The action is specified by default-action command.

Parameters *permit* — Specifies that packets matching the configured criteria will be permitted.

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

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

default-action

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

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

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

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

Default No default-action is defined.

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

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

dst-port

Syntax [**no**] **dst-port** *value* [*mask*]

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

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

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

Default No dst-port match criterion.

Parameters *value* — The source TCP or UDP port number as match criteria.

Values 1 — 65535 (decimal)

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

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

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

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

Default **65535** (exact match)

Values 1 — 65535 (decimal)

entry

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

Context config>system>security>mgmt-access-filter>ip-filter
config>system>security>mgmt-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 7750 SR OS exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.

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

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

Default No entries are defined.

Parameters *entry-id* — An entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries are numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.

Values 1 — 9999

flow-label

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

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

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

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

Values 0 — 1048575

log

Syntax [**no**] log

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

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

Default no log

next-header

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

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

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

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

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

protocol

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

Context config>system>security>mgmt-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, such as TCP, UDP, and OSPF, is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).

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

Default No protocol match criterion is specified.

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

Values 1 to 255 (decimal)

router

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

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

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

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

Parameters *router-instance* — Specify 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 — 2147483647

service-name *service-name* — Specifies an existing service name up to 64 characters in length.

renum

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

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

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

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

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

Values 1 — 9999

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

Values 1 — 9999

mac-filter

Syntax [**no**] **mac-filter**

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

Description This command configures a management access MAC-filter.

default-action

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

Context config>system>security>mgmt-access-filter>mac-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 No default-action is defined.

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

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

entry

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

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

Description This command matches criteria entry for the management-access-filter. Multiple entries can be created using unique entry-id numbers within the filter. The implementation exits the filter on the first match found and executes the actions in accordance with the accompanying 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** for it to be considered complete. Entries without the **action** keyword will be considered incomplete and hence will be rendered inactive.

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

Parameters *entry-id* — Specifies the MAC filter entry ID.

Values 1 — 9999

renum

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

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

Description This command remembers existing entries.

Parameters *old-entry-number* — Specifies the existing entry to renumber.

Values 1 — 9999

new-entry-number — Specifies the new entry number.

Values 1 — 9999

shutdown

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

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

Description This command shutdowns the management-access-filter.

action

Syntax **action deny**
action permit
no action

Context config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry

Description This command indicates the action to take when a packet matches this entry.

Parameters **deny —** Packets matching the configured criteria are denied and an ICMP host unreachable message is issued.

permit — Packets matching the configured criteria are permitted.

log

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

Context config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry

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

match

Syntax **match** [**frame-type** *frame-type*]
no match

Context config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry

Description This command configures math criteria for this MAC filter entry.

Parameters **frame-type** *frame-type* **—** Specifies the type of MAC frame to use as match criteria.

Values none, 802dot2-llc, ethernet_II

cfm-opcode

Syntax **cfm-opcode** {**lt | gt | eq**} *opcode*
cfm-opcode range *start end*
no cfm-opcode

Context config>system>security>mgmt-access-filter>mac-filter>entry
config>system>security>cpm-filter>mac-filter>entry>match

Description This command specifies the type of opcode checking to be performed.

If the cfm-opcode match condition is configured then a check must be made to see if the Ethertype is either IEEE802.1ag or Y1731. If the Ethertype does not match then the packet is not CFM and no match to the cfm-opcode is attempted.

The CFM (ieee802.1ag or Y1731) opcode can be assigned as a range with a start and an end number or with a (less than lt, greater than gt, or equal to eq) operator.

If no range with a start and an end or operator (lt, gt, eq) followed by an opcode with the value between 0 and 255 is defined then the command is invalid.

The following table provides opcode values.

Table 7: Opcode Values

CFM PDU or Organization	Acronym	Conflgurable Numeric Value (Range)
Reserved for IEEE 802.1 0		0
Continuity Check Message	CCM	1
Loopback Reply	LBR	2
Loopback Message	LBM	3
Linktrace Reply	LTR	4
Linktrace Message	LTM	5
Reserved for IEEE 802.1		6 – 31
Reserved for ITU		32
	AIS	33
Reserved for ITU		34
	LCK	35
Reserved for ITU		36
	TST	37
Reserved for ITU		38
	APS	39
Reserved for ITU		40
	MCC	41
	LMR	42
	LMM	43
Reserved for ITU		44
	1DM	45
	DMR	46
	DMM	47
Reserved for ITU		48 – 63
Reserved for IEEE 802.1 0		64 - 255

Defined by	ITU-T Y.1731	32 - 63
Defined by	IEEE 802.1.	64 - 255

Default no cfm-opcode

Parameters *opcode* — Specifies the opcode checking to be performed.

start — specifies the start number.

Values 0 — 255

end — Specifies the end number.

Values 0 — 255

lt|gt|eq — keywords

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures Dot1p match conditions.

Parameters *dot1p-value* — The IEEE 802.1p value in decimal.

Values 0 — 7

mask — This 3-bit mask can be configured using the following formats:

Values 0 — 7

dsap

Syntax **dsap** *dsap-value* [*dsap-mask*]

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures dsap match conditions.

Format Style	Format Syntax	Example
Decimal	`D`	`4`
Hexadecimal	`0xH`	`0x4`
Binary	`0bBBB`	`0b100`

Parameters *dsap-value* — The 8-bit dsap match criteria value in hexadecimal.

Values 0x00 — 0xFF (hex)

mask — This is optional and may be used when specifying a range of dsap values to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDD`	`240`
Hexadecimal	`0xHH`	`0xF0`
Binary	`0bBBBBBBBB`	`0b11110000`

Default FF (hex) (exact match)

Values 0x00 — 0xFF

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures the destination MAC match condition.

Parameters *ieee-address* — The MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

mask — A 48-bit mask to match a range of MAC address values.

etype

Syntax **etype** *0x0600xx0xffff*
no etype

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames, use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *ethernet-type* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 — 0xFFFF

snap-oui

Syntax **snap-oui** {**zero | non-zero**}

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame OUI zero or non-zero value to be used as a MAC filter match criterion.

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

Default no snap-oui

Parameters **zero —** Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.

snap-pid

Syntax **snap-pid** *snap-pid*
no snap-pid

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame PID value to be used as a MAC filter match criterion.

This is a two-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the three-byte OUI field.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

Note: The snap-pid match criterion is independent of the OUI field within the SNAP header. Two packets with different three-byte OUI fields but the same PID field will both match the same filter entry based on a snap-pid match criteria.

The **no** form of the command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *pid-value* — The two-byte snap-pid value to be used as a match criterion in hexadecimal.

Values 0x0000 — 0xFFFF

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Enter the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — This 48-bit mask can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default 0xFFFFFFFFFFFF (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>cpm-filter>mac-filter>entry>match

Description This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the Router Configuration Guide for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

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

Default no ssap

Parameters *ssap-value* — The 8-bit ssap match criteria value in hex.

Values 0x00 — 0xFF

ssap-mask — This is optional and may be used when specifying a range of ssap values to use as the match criteria.

svc-id

Syntax **svc-id** *service-id*
no svc-id

Context config>system>security>mgmt-access-filter>mac-filter>entry>match
config>system>security>mgmt-access-filter
config>system>security>mgmt-access-filter>ip-filter>entry
config>system>security>cpm-filter>mac-filter>entry>match

Description This command specifies an existing svc-id to use as a match condition.

Parameters *service-id* — Specifies a service-id to match.

Values		
	service-id:	1 — 2147483647
	svc-name:	64 characters maximum

src-port

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

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

Description This command restricts ingress management traffic to either the CPMEthernet port or any other logical port (LAG, 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 in the following format: slot[/mda]/port.

For example: To configure port 3 on MDA 2 on card 1 would be specified as 1/2/3.

Values	port-id	*slot*/*mda*/*port*[.*channel*]	
	encap-val	0	for null
		0 — 4094 for dot1q	
	aps-id	aps-*group-id*[.*channel*]	
	aps	keyword	
	group-id	1 — 64ccag-idccag-*id*. *path-id*[*cc-type*]	
		ccag	keyword
		id	1 — 8
		path-id	a, b
		cc-type	.sap-net, .net-sap
		cc-id	0 — 4094
	lag-id	lag-*id*	
		lag	keyword
		id	1 — 200
	cpm	keyword	

cpm — Configure the Ethernet port on the primary to match the criteria.

src-ip

Syntax [**no**] **src-ip** {[*ip-prefixImask*] **|** [*ip-prefix*]}

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

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

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

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

Default No source IP match criterion is specified.

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

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 **—** 32 (mask length), 0.0.0.0 **—** 255.255.255.255 (dotted decimal)

Password Commands

admin-password

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

Context config>system>security>password

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

This password is valid only for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.

This functionality can be enabled in two contexts:

config>system>security>password>admin-password

<global> enable-admin

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

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

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

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

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

Also note that usernames and passwords in the FTP and TFTP URLs will not be sent to the authorization or accounting servers when the **file>copy** *source-url dest-url* command is executed.

For example:

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

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

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

Default no admin-password

Parameters *password* — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

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

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

enable-admin

Syntax **enable-admin**

Context <global>

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

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

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

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

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

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

```
A:ALA-1# show users
===============================================================================
User Type From Login time Idle time
===============================================================================
admin Console -- 10AUG2006 13:55:24 0d 19:42:22
admin Telnet 10.20.30.93 09AUG2006 08:35:23 0d 00:00:00 A
-------------------------------------------------------------------------------
Number of users : 2
'A' indicates user is in admin mode
===============================================================================
A:ALA-1#
A:ALA-1# enable-admin
MINOR: CLI Already in admin mode.
A:ALA-1#
```

aging

Syntax **aging** *days*
no aging

Context config>system>security>password

Description This command configures the number of days a user password is valid before the user must change their password. This parameter can be used to force the user to change the password at the configured interval.

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

Default No aging is enforced.

Parameters *days* — The maximum number of days the password is valid.

Values 1 — 500

attempts

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

Context config>system>security>password

Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.

If the threshold is exceeded, the user is locked out for a specified time period.

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

The **no attempts** command resets all values to default.

Default **count**: **3**
time *minutes*: **5**
lockout *minutes*: **10**

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

Values 1 — 64

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

Values 0 — 60

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

Values 0 — 1440

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

Default 10

Values 0 — 1440

authentication-order

Syntax **authentication-order** [*method-1*] [*method-2*] [*method-3*] [**exit-on-reject**]
no authentication-order

Context config>system>security>password

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

The order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.

If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log register the failed attempt. Both the attempted login identification and originating IP address is logged with the a timestamp.

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

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

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

Default radius

Values radius, tacplus, local

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

Default tacplus

Values radius, tacplus, local

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

Default local

Values radius, tacplus, local

radius — RADIUS authentication.

tacplus — TACACS+ authentication.

local — Password authentication based on the local password database.

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

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

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

complexity

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

Context config>system>security>password

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

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

The **no** form of the command cancels all requirements. To remove a single requirement, enter the **no** form of the command followed by the requirement that needs to be removed.
For example, **no complexity numeric.**

Default No complexity requirements are configured.

Parameters **mixed-case —** Specifies that at least one upper and one lower case character must be present in the password. This keyword can be used in conjunction with the **numeric** and **special-character** parameters. However, if this command is used with the **authentication** *none* command, the **complexity** command is rejected.

numeric — Specifies that at least one numeric character must be present in the password. This keyword can be used in conjunction with the **mixed-case** and **special-character** parameters. However, if this command is used with the **authentication** *none* command, the **complexity** command is rejected.

special-character — Specifies that at least one special character must be present in the password. This keyword can be used in conjunction with the **numeric** and **special-character** parameters. However, if this command is used with the **authentication** *none* command, the **complexity** command is rejected.

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

health-check

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

Context config>system>security>password

Description This command specifies that RADIUS and TACACS+ servers are monitored for 3 seconds each at 30 second intervals. Servers that are not configured will have 3 seconds of idle time. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent.

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

Default health-check 30

Parameters **interval** *interval* **—** Specifies the polling interval for RADIUS servers.

Values 6 — 1500

minimum-length

Syntax **minimum-length** *value*
no minimum-length

Context config>system>security>password

Description This command configures the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the system security section.

If multiple minimum-length commands are entered each command overwrites the previous entered command.

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

Default **minimum-length 6**

Parameters *value* — The minimum number of characters required for a password.

Values 1 — 8

password

Syntax **password**

Context config>system>security

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

Public Key Infrastructure (PKI) Commands

pki

Syntax **pki**

Context config>system>security

Description This command enables the context to configure certificate parameters.

Default none

ca-profile

Syntax **ca-profile** *name* [**create**]
no ca-profile *name*

Context config>system>security>pki

Description This command creates a new **ca-profile** or enter the configuration context of an existing **ca-profile**. Up to 128 ca-profiles could be created in the system. A **shutdown** the ca-profile will not affect the current up and running **ipsec-tunnel** or **ipsec**-gw that associated with the **ca-profile**. But authentication afterwards will fail with a **shutdown ca-profile**.

Executing a **no shutdown** command in this context will cause system to reload the configured cert-file and crl-file.

A **ca-profile** can be applied under the **ipsec-tunnel** or **ipsec-gw** configuration.

The **no** form of the command removes the name parameter from the configuration. A ca-profile can not be removed until all the association(ipsec-tunnel/gw) have been removed.

Parameters *name* — Specifies the name of the **ca-profile**, a string up to 32 characters.

create — Keyword used to create a new **ca-profile**. The **create** keyword requirement can be enabled/ disabled in the **environment>create** context.

cert-file

Syntax **cert-file** *filename*
no cert-file

Context config>system>security>pki>ca-profile

Description Specifies the filename of a file in cf3:\system-pki\cert as the CA's certificate of the ca-profile.

Notes:

- The system will perform following checks against configured cert-file when a **no shutdown** command is issued:
  - → Configured cert-file must be a DER formatted X.509v3 certificate file.
  - → All non-optional fields defined in section 4.1 of RFC5280 must exist and conform to the RFC5280 defined format.
  - → Check The version field to see if its value is 0x2.
  - → Check The Validity field to see that if the certificate is still in validity period.
  - → X509 Basic Constraints extension must exists, and CA Boolean must be True.
  - → If Key Usage extension exists, then at least keyCertSign and cRLSign should be asserted.
  - → If the certificate is not a self-signing certificate , then system will try to look for issuer's CA's certificate to verify if this certificate is signed by issuer's CA; but if there is no such CA-profile configured, then system will just proceed with a warning message.
  - → If the certificate is not a self-signing certificate , then system will try to look for issuer's CA's CRL to verify that it has not been revoked; but if there is no such CA-profile configured or there is no such CRL, then system will just proceed with a warning message.

  If any of above checks fails, then the "no shutdown" command will fails.
- Changing or removing of **cert-file** is only allowed when the **ca-profile** is in a **shutdown** state.

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

Parameters *filename* — Specifies a local CF card file URL

crl-file

Syntax **crl-file** *filename*
no crl-file

Context config>system>security>pki>ca-profile

Description This command specifies the name of a file in cf3:\system-pki\crl as the Certification Revoke List file of the **ca-profile**.

Notes:

- The system will perform following checks against configured crl-file when a **no shutdown** command is issued:
  - → A valid cert-file of the ca-profile must be already configured.
  - → Configured crl-file must be a DER formated CRLv2 file.
  - → All non-optional fields defined in section 5.1 of RFC5280 must exist and conform to the RFC5280 defined format.
  - → Check the version field to see if its value is 0x1.
  - → Delta CRL Indicator must NOT exists (delta CRL is not supported).
  - → CRL's signature must be verified by using the cert-file of ca-profile.

If any of above checks fail, the **no shutdown** command will fail.

- Changing or removing the **crl-file** is only allowed when the **ca-profile** is in a **shutdown** state.

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

Default none

Parameters *filename* — Specifies the name of CRL file stored in cf3:\system-pki\crl.

maximum-cert-chain-depth

Syntax **maximum-cert-chain-depth** *level*
no maximum-cert-chain-depth

Context config>system>security>pki

Description This command defines the maximum depth of certificate chain verification. This number is applied system wide.

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

Default 7

Parameters *level* — Specifies the maximum depth level of certificate chain verification, range from 1 to 7. the certificate under verification is not counted in. for example, if this parameter is set to 1, then the certificate under verification must be directly signed by trust anchor CA.

Values 1 — 7

shutdown

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

Context config>system>security>pki>ca-profile>

Description Use this command to enable or disable the ca-profile. The system will verify the configured cert-file and crl-file. If the verification fails, then the **no shutdown** command will fail.

The ca-profile in a **shutdown** state cannot be used in certificate authentication.

Default shutdown

http-download

Syntax **http-download** *http-url* **to** *local-url* **router** {**base**|**management**} [**force**]

Context file

Description This is a file utility command to download files via the HTTP protocol. This command works with both IPv4 and IPv6. Use the **config>system>dns>address-pref** command to decide the protocol preference.

Default none

Parameters *local-file-url* — Specifies the local CF card path and filename to save

remote-url — Specifies an http URL to download file from, has the format of http://username:password@remote-url, username and password are used when HTTP server require basic or digest access authentication.

router — Specifies the router instance that is applicable for the HTTP download.

force — With this parameter, the existing local file will be overwritten without confirmation; otherwise system will promote for confirmation if a local file with the same path/name already exists.

certificate

Syntax **certificate**

Context admin

Description This command enables the context to configure X.509 certificate related operational parameters.

display

Syntax **display type** {**cert|key|crl|cert-request**} *url-string* **format** {**pkcs10|pkcs12|pkcs7-der|pkcs7-pem|pem|der**} [**password** [*32 chars max*]]

Context admin>certificate

Description This command displays the content of an input file in plain text. Note that when displaying the key file content, only the key size and type are displayed.

The following list summarizes the formats supported by this command:

- Certificate
  - → 7750 system format
  - → PKCS #12
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → RFC4945
- Certificate Request
  - → PKCS #10
- Key
  - → 7750 system format

  - → PKCS #12
- CRL
  - → 7750 system format
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → RFC4945

Default none

Parameters *file-url* — Specifies the local CF card url of the input file.

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

type — Specifies the type of input file, possible values are cert/key/crl/cert-request.

Values cert, key, crl, cert-request

format — Specifies the format of input file.

Values pkcs10, pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is a encrypted PKCS#12 file, up to 99 characters in length.

export

Syntax **export type** {**cert**|**key**|**crl**} **input** *filename* **output** *url-string* **format** *output-format* [**password** [*32 chars max*]] [**pkey** *filename*]

Context admin>certificate

Description

gen-keypair

Syntax **gen-keypair** *url-string* [**size** {**512**|**1024**|**2048**}] [**type** {**rsa**|**dsa**}]

Context admin>certificate

Description This command generatse a RSA or DSA private key/public key pairs and store them in a local file in cf3:\system-pki\key

Parameters *url-string* — Specifies the name of the key file.

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

size — Specifies the key size in bits.

possible choice are 512/1024/2048; the default value is

Default 2048

type — Specifies the type of key.

Default rsa

gen-local-cert-req

Syntax **gen-local-cert-req keypair** *url-string* **subject-dn** *subject-dn* [**domain-name** [*255 chars max*]] [**ip-addr** *ip-address*] **file** *url-string*

Context admin>certificate

Description This command generate a PKCS#10 formatted certificate request by using a local existing key pair file.

Default none

Parameters *url-string* — Specifies the name of the keyfile in cf3:\system-pki\key that used to generate certificate request.

Values		
	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

subject-dn — Specifies the distinguish name that used as subject in certificate request, including:

- C-Country
- ST-State
- O-Organization name
- OU-Organization Unit name
- CN-common name

This parameter is formatted as a text string includes any of above attributes, the attribute and its value is linked by using “=”, and “,” is used to separate different attributes.

For example: C=US,ST=CA,O=ALU,CN=7750 SR12

Values attr1=val1,attr2=val2... where: attrN={C|ST|O|OU|CN}, 256 chars max

domain-name — optionally, a domain name string can be specified and included as dNSName in Subject Alternative Name extension of the certificate request.

ip-address — optionally, an IPv4 address string can be specified and included as ipAddress in Subject Alternative Name extension of the certificate request.

cert-req-file-url — this url could be either a local CF card path and filename to save the certificate request; or a FTP url to upload the certificate request.

import

Syntax **import type** {**cert**|**key**|**crl**} **input** *url-string* **output** *filename* **format** *input-format* [**password** [*32 chars max*]]

Context admin>certificate#

Description This command converts an input file(key/certificate/CRL) to a 7750 system format file. The following list summarizes the formats supported by this command:

- Certificate
  - → PKCS #12
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → PEM
  - → DER
- Key
  - → PKCS #12
  - → PEM
  - → DER
- CRL
  - → PKCS #7 PEM encoded
  - → PKCS #7 DER encoded
  - → PEM
  - → DER

Note that if there are multiple objects with same type in the input file, only first object will be extracted and converted.

Default none

Parameters **input** *url-string* **—** Specifies the URL for the input file. This URL could be either a local CF card URL file or a FP URL to download the input file.

output *url-string* **—** Specifies the name of output file up to 95 characters in length. The output directory depends on the file type like following:

- Key: cf3:\system-pki\key
- Cert: cf3:\system-pki\cert
- CRL: cf3:\system-pki\CRL

Values	url-string	<local-url> - [99 chars max]
	local-url	<cflash-id>/<file-path>
	cflash-id	cf1:|cf2:|cf3:

type **—** The type of input file.

Values cert, key, crl

format — Specifies the format of input file.

Values pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is a encrypted PKCS#12 file.

reload

Syntax **reload type** {**cert**|**key**} *filename*

Context admin>certificate

Description This command reloads the certificate/key file.

Parameters *filename* — Specifies the file name up to 95 characters in length.

Profile Management Commands

action

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

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

Description This command configures the action associated with the profile entry.

Parameters **deny —** Specifies that commands matching the entry command match criteria are to be denied.

permit — Specifies that commands matching the entry command match criteria will be permitted.

match

Syntax **match** *command-string*
no match

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

Description This command configures a command or subtree commands in subordinate command levels are specified.

Because the 7750 SR exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile.

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

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

Default none

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

copy

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

Context config>system>security

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

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

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

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

default-action

Syntax **default-action** {**deny-all | permit-all | none}**

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

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

Default none

Parameters **deny-all —** Sets the default of the profile to deny access to all commands.

permit-all — Sets the default of the profile to permit access to all commands.

Note: permit-all does not change access to security commands. Security commands are only and always available to members of the super-user profile.

none — Sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user.

For example, if a user is a member of two profiles and the default action of the first profile is **permit-all**, then the second profile will never be evaluated because the **permit-all** is executed first. Set the first profile default action to **none** and if no match conditions are met in the first profile, then the second profile will be evaluated. If the default action of the last profile is **none** and no explicit match is found, then the default **deny-all** takes effect.

description

Syntax **description** *description-string*
no description

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

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

The **description** command associates a text string with a configuration context to help identify the context in the configuration file.

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

Default No description is configured.

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

entry

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

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

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

More than one entry can be created with unique *entry-id* numbers. Exits when the first match is found and executes the actions according to the accompanying **action** command. Entries should be sequenced from most explicit to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** for it to be considered complete.

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

Default No entry IDs are defined.

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

Values 1 — 9999

profile

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

Context config>system>security

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

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

Once the profiles are created, the **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 *user-profile-name* can consist of up to 32 alphanumeric characters.

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

Default user-profile default

Parameters *user-profile-name* — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

renum

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

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

Description This command renumbers profile entries to re-sequence the entries.

Since the 7750 SR exits when the first match is found and executes the actions according to accompanying action command, re-numbering is useful to rearrange the entries from most explicit to least explicit.

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

Values 1 — 9999

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

Values 1 — 9999

User Management Commands

access

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

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

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

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

The **no** form of command removes access for a specific application.
no access denies permission for all management access methods. To deny a single access method, enter the **no** form of the command followed by the method to be denied, for example, **no access FTP** denies FTP access.

Default No access is granted to the user by default.

Parameters **ftp —** Specifies FTP permission.

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

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

li — Allows user to access CLI commands in the lawful intercept (LI) context.

authentication

Syntax **authentication** {[**none**] | [[**hash**] {**md5** *key-1* **| sha** *key-1*} **privacy** {**none|des-key|aes-128-cfb-key** *key-2*}]

Context config>system>security>user>snmp

Description This command configures the authentication and encryption method the user must use in order to be validated by the 7750 SR device. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered.

The **user password** is encrypted first by the MD5/SHA/DES algorithm. The output of the algorithm is always a fixed length string (key). Copy the **password** key and paste the output in the appropriate **authentication** command *key* parameter.

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

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

hash — When **hash** is not specified, then non-encrypted characters can be entered. When **hash** is configured, then all specified keys are stored in an encrypted format in the configuration file. The password must be entered in encrypted form when the **hash** parameter is used.

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

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

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

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

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

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

privacy none — Do not perform SNMP packet encryption.

Default privacy none

privacy des-key key-2 — Use DES for SNMP payload encryption and configure the key. The key must be a 32 hex-character string and is stored in an encrypted format.

privacy aes-128-cfb-key key-2 — Use 128 bit CFB mode AES for SNMP payload encryption and configure the key. The key must be a 32 hex-character string and is stored in an encrypted format.

Default privacy none

group

Syntax **group** *group-name*
no group

Context config>system>security>user>snmp

Description This command associates (or links) a user to a group name. The group name must be configured with the **config>system>security>user >snmp>group** command. The **access** command links the group with one or more views, security model (s), security level (s), and read, write, and notify permissions

Default No group name is associated with a user.

Parameters *group-name* — Enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group-name per security model.

cannot-change-password

Syntax [**no**] **cannot-change-password**

Context config>system>security>user>console

Description This command allows a user the privilege to change their password for both FTP and console login.

To disable a user’s privilege to change their password, use the **cannot-change-password** form of the command.

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

Default no cannot-change-password

console

Syntax **console**

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

Description This command creates the context to configure user profile membership for the console (either Telnet or CPM serial port user).

copy

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

Context config>system>security

Description This command copies a specific user’s configuration parameters to another (destination) user.

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

Parameters *source-user* — The user to copy. The user must already exist.

dest-user — The copied profile is copied to a destination user.

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

home-directory

Syntax **home-directory** *url-prefix* [*directory*] [*directory***/***directory…*]
no home-directory

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

Description This command configures the local home directory for the user for both console and FTP access.

If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed.

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

Default no home-directory

NOTE: If restrict-to-home has been configured no file access is granted and no home-directory is created, if restrict-to-home is not applied then root becomes the user's home-directory.

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

profile

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

Context config>system>security>user-template

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

Parameters *user-profile-name* — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

login-exec

Syntax [**no**] **login-exec** *url-prefix*: *source-url*

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

Description This command configures a user's login exec file which executes whenever the user successfully logs in to a console session.

Only one exec file can be configured. If multiple **login-exec** commands are entered for the same user, each subsequent entry overwrites the previous entry.

The **no** form of the command disables the login exec file for the user.

Default No login exec file is defined.

Parameters *url-prefix: source-url* — Enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that will be executed after the user successfully logs in.

member

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

Context config>system>security>user>console

Description This command is used to allow the user access to a profile.

A user can participate in up to eight profiles.

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

Default default

Parameters *user-profile-name* — The user profile name.

new-password-at-login

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

Context config>system>security>user>console

Description This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login.

The **no** form of the command does not force the user to change passwords.

Default no new-password-at-login

password

Syntax **password** [*password*] [**hash | hash2**]

Context config>system>security>user

Description This command configures the user password for console and FTP access.

The use of the **hash** keyword sets the initial password when the user is created or modifies the password of an existing user and specifies that the given password was hashed using hashing algorithm version 1.

The password is stored in an encrypted format in the configuration file when specified. Passwords should be encased in double quotes (" ") at the time of the password creation. The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

The use of the **hash2** keyword specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify if it is a valid hash 2 key to store in the database.

In previous releases, the **password** command syntax included the hash (hash version 1) parameter that allowed you to specify a password and encryption. For example,

```
config>system>security>user# password testuser1
```

The password was hashed by default.

For example:

```
config>system>security# user testuser1
config>system>security>user$ password xyzabcd1
config>system>security>user# exit


config>system>security# info
-------------------------------------
...
            user "testuser1"
                password "I/VhQSk/FWY" hash
            exit
...
-------------------------------------
config>system>security#
```

In the current release, the **password** command allows you also to specify a different hashing scheme, hash version 2.

For example,

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

config>system>security# info
-------------------------------------
...
            user "testuser1"
                password "zx/Uhcn6ReMOZ3BVrWcvk." hash2
            exit
...
-------------------------------------
config>system>security#
```

Parameters

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

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

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

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

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

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

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

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

restricted-to-home

Syntax [**no**] **restricted-to-home**

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

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

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

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

Default no restricted-to-home

snmp

Syntax **snmp**

Context config>system>security>user

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

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

7750 SR OS always uses the configured SNMPv3 user name as the security user name.

user-template

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

Context config>system>security

Description This command configures default security user template parameters.

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

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

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

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

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

Default none

Parameters *user-name* — The name of the user up to 16 characters.

RADIUS Client Commands

access-algorithm

Syntax **access-algorithm** {**direct | round-robin**}
no access-algorithm

Context config>system>security>radius

Description This command indicates the algorithm used to access the set of RADIUS servers.

Default direct

Parameters **direct —** The first server will be used as primary server for all requests, the second as secondary and so on.

round-robin — The first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

accounting

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

Context config>system>security>radius

Description This command enables RADIUS accounting.

The **no** form of this command disables RADIUS accounting.

Default no accounting

accounting-port

Syntax **accounting-port** *port*
no accounting-port

Context config>system>security>radius

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

Parameters *port* — Specifies the UDP port number.

Values 1 — 65535

Default 1813

authorization

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

Context config>system>security>radius

Description This command configures RADIUS authorization parameters for the system.

Default no authorization

port

Syntax **port** *port*
no port

Context config>system>security>radius

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

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

Default **1812** (as specified in RFC 2865, *Remote Authentication Dial In User Service* (*RADIUS*))

Parameters *port* — The TCP port number to contact the RADIUS server.

Values 1 — 65535

radius

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

Context config>system>security

Description This command creates the context to configure RADIUS authentication on the 7750 SR-Series router.

Implement redundancy by configuring multiple server addresses for each 7750 SR-Series router.

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

retry

Syntax **retry** *count*
no retry

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

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

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

Default 3

Parameters *count* — The retry count.

Values 1 — 10

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2**]
no server *index*

Context config>system>security>radius

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

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

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

Default No RADIUS servers are configured.

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

Values 1 — 5

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

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

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

Values Up to 128 characters in length.

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

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

shutdown

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

Context config>system>security>radius

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

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

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

Default no shutdown

timeout

Syntax **timeout** *seconds*
no timeout

Context config>system>security>radius

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

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

Default 3 seconds

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

Values 1 — 90

use-default-template

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

Context config>system>security>radius

Description This command specifies whether the RADIUS user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the RADIUS user template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server.

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

TACACS+ Client Commands

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**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 lowest index to the highest index for authentication requests.

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

Default No TACACS+ servers are configured.

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

Values 1 — 5

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

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

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

Values Up to 128 characters in length.

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

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

port *port* **—** Specifies the port ID.

Values 0 — 65535

shutdown

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

Context config>system>security>tacplus

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

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

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

Default no shutdown

tacplus

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

Context config>system>security

Description This command creates the context to configure TACACS+ authentication on the 7750 SR-Series router.

Configure multiple server addresses for each 7750 SR-Series router for redundancy.

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

accounting

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

Context config>system>security>tacplus

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

Default record-type stop-only

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

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

authorization

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

Context config>system>security>tacplus

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

Default no authorization

timeout

Syntax **timeout** *second*s
no timeout

Context config>system>security>tacplus

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

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

Default **3**

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

Values 1 — 90

shutdown

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

Context config>system>security>tacplus

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

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

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

Default no shutdown

use-default-template

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

Context config>system>security>tacplus

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

Generic 802.1x COMMANDS

dot1x

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

Context config>system>security

Description This command creates the context to configure 802.1x network access control on the 7750 SR OS router.

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

radius-plcy

Syntax [**no**] **radius-plcy**

Context config>system>security> dot1x

Description This command creates the context to configure RADIUS server parameters for 802.1x network access control on the 7750 SR router.

NOTE: The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the 7750 SR as opposed to the RADIUS server configured under the **config>system>radius** context which authenticates CLI login users who get access to the management plane of the 7750 SR.

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

retry

Syntax **retry** *count*
no retry

Context config>system>security> dot1x

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

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

Default 3

Parameters *count* — The retry count.

Values 1 — 10

server (dot1x)

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

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

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

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

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

Default No Dot1x servers are configured.

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

Values 1 — 5

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

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

Values Up to 128 characters in length.

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

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

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

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

Values 1 — 65535

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

Values authorization, accounting, combined

source-address

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

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

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

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

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

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

Values 0.0.0.0 — 255.255.255.255

shutdown

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

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

Description This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

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

Default shutdown

timeout

Syntax **timeout** *seconds*
no timeout

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

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

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

Default 3 seconds

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

Values 1 — 90

TCP Enhanced Authentication

keychain

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

Context config>system>security

Description This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

The **no** form of the command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.

Default none

Parameters *keychain-name* — Specifies a keychain name which identifies this particular keychain entry.

Values An ASCII string up to 32 characters.

direction

Syntax **direction**

Context config>system>security>keychain

Description This command specifies the data type that indicates the TCP stream direction to apply the keychain.

Default none

bi

Syntax **bi**

Context config>system>security>keychain>direction

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

Default none

uni

Syntax **uni**

Context config>system>security>keychain>direction

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

Default none

receive

Syntax **receive**

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

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

Default none

send

Syntax **send**

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

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

Default none

entry

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

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

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

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

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

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

Default There are no default entries.

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

Values 0 — 63

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

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

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

Values A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.

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

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

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

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

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

hash2 — Specifies the key is entered in a more complex encrypted form.

begin-time

Syntax **begin-time** [*date] [hours-minutes*] [**UTC**] [**now**] [**forever**]

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

Description This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.

If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.

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

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

now — Specifies the the key should become active immediately.

forever — Specifies that the key should always be active.

end-time

Syntax **end-time** [*date] [hours-minutes*] [**UTC**] [**now**] [**forever**]

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

Description This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream.

Default forever

Parameters *date* — Specifies the calendar date after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the YYYY/MM/DD format. When no year is specified the system assumes the current year.

hours-minutes — Specifies the time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the hh:mm[:ss] format. Seconds are optional, and if not included, assumed to be 0.

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

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

forever — Specifies a time beyond the current epoch.

tolerance

Syntax **tolerance** [*seconds* **| forever**]

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

Description This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.

Parameters *seconds* — Specifies the duration that an eligible receive key overlaps with the active send key.

Values 0 — 4294967294 seconds

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

tcp-option-number

Syntax **tcp-option-number**

Context config>system>security>keychain

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

receive

Syntax **receive** *option-number*

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

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

Default 254

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

Values 253, 254, 253&254

send

Syntax **send** *option-number*

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

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

Default 254

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

Values 253, 254

CPM Filter Commands

cpm-filter

Syntax **cpm-filter**

Context config>system>security

Description This command enables the context to configure a CPM filter. A CPM filter is a hardware filter done by the P chip on the CPMCFM that applies to all the traffic going to the CPM CPU. It can be used to drop, accept packets, as well as allocate dedicated hardware queues for the traffic.

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 take on the traffic when the filter entry matches. If there are no filter entry defined, the packets received will either be dropped or forwarded based on that default action.

Default accept

Parameters **accept —** Specfies that packets matching the filter entry are forwarded.

drop — Specifies that packets matching the filter entry are dropped.

ip-filter

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

Context config>system>security>cpm-filter

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

Default shutdown

ipv6-filter

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

Context config>system>security>cpm-filter

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

Default shutdown

entry

Syntax **entry** *entry-id*

Context config>sys>sec>cpm>ip-filter
config>sys>sec>cpm>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 will match every packet, and the entry action will be taken. Entries are created and deleted by user.

Parameters *entry-id* — Identifies a CPM filter entry as configured on this system.

Values 1 — 2048

action

Syntax **action [accept | drop | queue** *queue-id]*
no action

Context config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry

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

Default drop

Parameters **accept —** Specifies packets matching the entry criteria will be forwarded.

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

queue *queue-id* **—** Specifies packets matching the entry criteria will be forward to the specified CPM hardware queue.

log

Syntax **log** *log-id*

Context config>sys>sec>cpm>ip-filter>entry
config>sys>sec>cpm>ipv6-filter>entry

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

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

Parameters *log-id* — Specifies the log ID where packets matching this entry should be entered.

match

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

Context config>sys>sec>cpm>ip-filter>entry

Description This command enables the context to enter match criteria for the filter entry. When the match criteria have been satisfied the action associated with the match criteria is executed. If more than one match criteria (within one match statement) are configured then 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.

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

Parameters **protocol —** Configures an IP protocol to be used as an IP filter match criterion. The protocol type such as TCP or UDP is identified by its respective protocol number.

protocol-id — Configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the match criteria.

Values 1 — 255 (values can be expressed in decimal, hexidecimal, or binary)
keywords - none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp , * — udp/tcp wildcard

Table 8: IP Protocol Names

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	any private interior gateway (used by Cisco for their IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6

Table 8: IP Protocol Names (Continued)

Protocol	Protocol ID	Description
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>sys>sec>cpm>ipv6-filter>entry

Description This command specifies match criteria for the IP filter entry.

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

Parameters **next-header** *next-header* — Specifies the next header to match.

The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).

Values next-header: 1 — 42, 45— 49, 52— 59, 61— 255 protocol numbers accepted in DHB
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

dscp

Syntax **dscp** *dscp-name*
no dscp

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>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** — No dscp match criterion.

Parameters *dscp-name* — Configures a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point may only be specified by its name.

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address netmask*}
no dst-ip

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures a destination IP address range to be used as an IP filter match criterion.

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 may also be used.

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

Default No destination IP match criterion

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

Values 0.0.0.0 — 255.255.255.255

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 — 32

netmask — Specifies the dotted quad equivalent of the mask length.

Values 0.0.0.0 — 255.255.255.255

dst-ip

Syntax **dst-ip** [*ipv6-address /prefix-length*]
no dst-ip

Context config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures a destination IPv6 address range to be used as an IPv6 filter match criterion.

To match on the destination IPv6 address, specify the address.

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

Default No destination IP match criterion

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 1010::700:0:217A is the same as 1010:0:0:0:0:700:0:217A.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 — .FFFF]H
d: [0 — 255]D
prefix-length: 1 — 128

dst-port

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

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

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

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

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

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

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

flow-label

Syntax **flow-label** *value*

no flow-label

Context config>sys>sec>cpm>ipv6-filter>entry>match

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

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

Values 0 — 1048575

fragment

Syntax **fragment** {**true | false**}
no fragment

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures fragmented or non-fragmented IP packets as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default **no fragment**

Parameters **true —** Configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set OR have the Fragment Offset field of the IP header set to a non-zero value.

false — 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>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on ICMP code field in the ICMP header of an IP packet as an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The behavior of the **icmp-code** value is dependent on the configured **icmp-type** value, thus a configuration with only an **icmp-code** value specified will have no effect. To match on the **icmp-code**, an associated **icmp-type** must also be specified.

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

Default **no icmp-code** - no match criterion for the ICMP code.

Parameters *icmp-code* — Specifies the ICMP code values that must be present to match.

Values 0 — 255

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command configures matching on ICMP type field in the ICMP header of an IP packet as an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default **no icmp-type** — No match criterion for the ICMP type.

Parameters *icmp-type* — Specifies the ICMP type values that must be present to match.

Values 0 — 255

ip-option

Syntax **ip-option** *ip-option-value ip-option-mask*
no ip-option

Context config>sys>sec>cpm>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.

Default No IP option match criterion

Parameters *ip-option-value* — Enter the 8 bit option-type as a decimal integer. The mask is applied as an AND to the option byte, the result is compared with the option-value.

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

Values 0 — 255

ip-option-mask — Specifies a range of option numbers to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDD`	`20`
Hexadecimal	`0xHH`	`0x14`
Binary	`0bBBBBBBBB`	`0b0010100`

Default 255 (decimal) (exact match)

Values 1 — 255 (decimal)

multiple-option

Syntax **multiple-option** {**true | false**}
no multiple-option

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures matching packets that contain more than one option fields 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.

Default **no multiple-option** — No checking for the number of option fields in the IP header

Parameters **true —** Specifies matching on IP packets that contain more that one option field in the header.

false — Specifies matching on IP packets that do not contain multiple option fields present in the header.

option-present

Syntax **option-present** {**true | false**}
no option-present

Context config>sys>sec>cpm>ip-filter>entry>match

Description This command configures matching packets that contain the option field or have an option field of zero 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.

Parameters **true —** Specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of zero 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 zero). An option field of zero is considered as no option present.

router

Syntax **router service-name** *service-name*
router *router-instance*
no router

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies a router name or a service-id to be used in the match criteria.

Parameters *router-instance* — Specify 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 — 2147483647

service-name *service-name* — Specifies an existing service name up to 64 characters in length.

src-ip

Syntax **src-ip** [*ip-address/mask*]
no src-ip

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command specifies the IP or IPv6 address to match the source IP or or IPv6 address of the packet.

To match on the source IP address, specify the address and its associated mask, such as 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

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

Default **no src-ip** — No source IP match criterion.

Parameters *ip-address/mask* — Specifies the IP address for the match criterion in dotted decimal notation. An IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 1010::700:0:217A is the same as 1010:0:0:0:0:700:0:217A.

Values	ipv4-address	a.b.c.d (host bits must be 0)
	ipv6-address	x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses
	mask:	Specifies the 16 bit mask to be applied when matching the source IP address. 1 — 32

src-port

Syntax **src-port** *src-port-number* [*mask*]

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match

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

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

Values 0 — 65535

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

Values 0 — 128

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>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 or IPv6 packet as an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default No match criterion for the ACK bit

Parameters **true —** Specifies matching on IP or IPv6 packets that have the ACK bit set in the control bits of the TCP header of an IP or IPv6 packet.

false — Specifies matching on IP or IPv6 packets that do not have the ACK bit set in the control bits of the TCP header of the IP or IPv6 packet.

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context config>sys>sec>cpm>ip-filter>entry>match
config>sys>sec>cpm>ipv6-filter>entry>match
config>sys>sec>cpm>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 or IPv6 packet as an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP or IPv6 address.

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

Default No match criterion for the SYN bit

Description Use the no form of this command to remove this as a criterion from the match entry.

Default none

Parameters **true —** Specifies matching on IP or IPv6 packets that have the SYN bit set in the control bits of the TCP header.

false — Specifies matching on IP or IPv6 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>sys>sec>cpm>ip-filter
config>sys>sec>cpm>ipv6-filter>entry>match

Description This command renumbers existing IP or IPv6 filter entries to re-sequence filter entries.

This may be required in some cases since the OS exits when the first match is found and execute the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

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

Values 1 — 2048

new-entry-id — Enter the new entry-number to be assigned to the old entry.

Values 1 — 2048

CPM Queue Commands

cpm-queue

Syntax **cpm-queue**

Context config>system>security

Description This command enables the context to configure a CPM queue.

queue

Syntax **queue** *queue-id*

Context config>system>security>cpm-queue

Description This command allows users to allocate dedicated CPM.

cbs

Syntax **cbs** *cbs*
no cbs

Context config>system>cpm-queue>queue

Description This command specifies the amount of buffer that can be drawn from the reserved buffer portion of the queue's buffer pool.

Parameters *cbs* — Specifies the commited burst size in kbytes.

mbs

Syntax **mbs** *mbs*
no mbs

Context config>system>security>cpm-queue>queue

Description This command specifies the maximum queue depth to which a queue can grow.

Parameters *mbs* — Specifies the maximum burst size in kbytes.

rate

Syntax **rate** *rate* [**cir** *cir*]
no rate

Context config>system>security>cpm-queue>queue

Description This command specifies the maximum bandwidth that will be made available to the queue in kilobits per second (kbps).

Parameters *rate* — Specifies the administrative Peak Information Rate (PIR) for the queue.

cir *cir* **—** Specifies the amount of bandwidth committed to the queue.

TTL Security Commands

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>router>bgp>group
config>router>bgp>group>neighbor

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, LDP 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. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming BGP packet.

Values 1 — 255

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>router>ldp>peer-parameters>peer

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, BGP 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. Per-peer-queueing must be enabled in order for TTL protection to operate.

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 LDP packet.

Values 1 — 255

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>system>login-control>ssh config>system>login-control>telnet

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, SSH/Telnet 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. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming BGP packet.

Values 1 — 255

CPU Protection Commands

cpu-protection

Syntax **cpu-protection**

Context config>sys>security

Description This command enters the context to configure CPU protection parameters.

link-specific-rate

Syntax **link-specific-rate** *packet-rate-limit*
no link-specific-rate

Context config>sys>security>cpu-protection

Description This command configures a link-specific rate for CPU protection. This limit is applied to all ports within the system. The CPU will receive no more than the configured packet rate for all link level protocols such as LACP from any one port. The measurement is cleared each second and is based on the ingress port.

Default max (no limit)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit, in packets per second, for link level protocols.

Values 1 — 65535, max (no limit)

policy

Syntax **policy** *cpu-protection-policy-id* [**create**]
no policy *cpu-protection-policy-id*

Context config>sys>security>cpu-protection

Description This command configures CPU protection policies.

The **no** form of the command deletes the specified policy from the configuration.

Policies 254 and 255 are reserved as the default access and network interface policies, and cannot de deleted. The parameters within these policies can be modified. An event will be logged (warning) when the default policies are modified.

Default Policy 254 (default access interface policy):

per-source-rate: max (no limit)

overall-rate : 6000

out-profile–rate: 6000

alarm

Policy 255 (default network interface policy):

per-source-rate: max (no limit)

overall-rate : max (no limit)

out-profile-rate: 3000

alarm

Parameters *cpu-protection-policy-id* — Assigns a policy ID to the specific CPU protection policy.

Values 1 — 255

create — Keyword used to create CPU protection policy. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

alarm

Syntax [**no**] **alarm**

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

Description This command enables the generation of an event that includes information about the protocol, the offending source and the measured rate. Only one event is generated per monitor period.

The **no** form of the command disables the notifications.

Default no alarm

eth-cfm

Syntax **eth-cfm**
no eth-cfm

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

Description Provides the construct under which the different entries within CPU policy can define the match criteria and overall arrival rate of the Ethernet Configuration and Fault Management (ETH-CFM) packets at the CPU.

Default None

entry

Syntax **entry** *<entry>* **levels** *<levels>* **opcodes** *<opcodes>* **rate** *<packet-rate-limit>*
no entry

Context config>sys>security>cpu-protection>eth-cfm>

Description Builds the specific match and rate criteria. Up to ten entries may exist in up to four CPU protection policies.

The **no** form of the command reverses the match and rate criteria configured.

Default no entry

Parameters **rate —** Specifies a packet rate limit in frames per second, where a ‘0’ means drop all.

Values 1 —100

level — Specifies a domain level.

Values		
	all	Wildcard entry level
	range	0 —7: within specified range, multiple ranges allowed
	number	0 ... 7: specific level number, may be combined with range

opcode — Specifies an operational code that identifies the application.

Values		
	range	0 —255: within specified range, multiple ranges allowed
	number	0 .. .255: specific level number, may be combined with range

out-profile-rate

Syntax **out-profile-rate** *packet-rate-limit*
no out-profile-rate

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

Description This command applies a packet arrival rate limit for the entire SAP/interface, above which packets will be market as discard eligible. The rate defined is a global rate limit for the interface regardless of the number of subscribers or hosts are present on the SAP/interface. It is a per-SAP/interface rate.

The **no** form of the command sets out-profile-rate parameter back to the default value.

Default **3000** for cpu-protection-policy-id 1-253

6000 for cpu-protection-policy-id 254 (default access interface policy)

3000 for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

overall-rate

Syntax **overall-rate** *packet-rate-limit*
no overall-rate

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

Description This command applies a maximum packet arrival rate limit (applied per SAP/interface) for the entire SAP/interface, above which packets will be discarded immediately. The rate defined is a global rate limit for the interface regardless of how many subscribers or hosts are present on the SAP/interface. It is a per-SAP/interface rate.

The **no** form of the command sets overall-rate parameter back to the default value.

Default **max** for cpu-protection-policy-id 1 — 253

6000 for cpu-protection-policy-id 254 (default access interface policy)

max for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

per-source-rate

Syntax **per-source-rate** *packet-rate-limit*
no per-source-rate

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

Description This command configures a per-source packet arrival rate limit. Use this command to apply a packet arrival rate limit on a per source basis. A source is defined as a unique combination of SAP and MAC source address (mac-monitoring) or SAP and source IP address (ip-src-monitoring). The CPU will receive no more than the configured packet rate from each source (only the DHCP protocol is rate limited for ip-src-monitoring). the measurement is cleared each second.

This parameter is only applicable if the policy is assigned to an interface (some examples include saps, subscriber-interfaces, and spoke-sdps), and the **mac-monitor** or **ip-src-monitor** keyword is specified in the **cpu-protection** configuration of that interface.

Default max, no limit

Parameters *packet-rate-limit* — Specifies a per-source packet (per SAP/MAC souce address or per SAP/IP source address) arrival rate limit in packets per second.

Values 1 — 65535, max (max indicates no limit)

port-overall-rate

Syntax **port-overall-rate** *packet-rate-limit*
no port-overall-rate

Context config>sys>security>cpu-protection

Description This command configures a per-port overall rate limit for CPU protection.

Parameters *packet-rate-limit* — Specifies an overall per-port packet arrival rate limit in packets per second.

Values 1 — 65535, max (indicates no limit)

protocol-protection

Syntax **protocol-protection** [**allow-sham-links**]
no protocol-protection

Context config>sys>security>cpu-protection

Description This command causes the network processor on the CPM to discard all packets received for protocols that are not configured on the particular interface. This helps mitigate DoS attacks by filtering invalid control traffic before it hits the CPU. For example, if an interface does not have IS-IS configured, then protocol protection will discard any IS-IS packets received on that interface.

Default no protocol-protection

Parameters **allow-sham-links —** Allows sham links. As OSPF sham links form an adjacency over the MPLS-VPRN backbone network, when protocol-protection is enabled, the tunneled OSPF packets to be received over the backbone network must be explicitly allowed.

cpu-protection

Syntax **cpu-protection** *policy-id*
no cpu-protection

Context config>router>interface
config>service>ies>interface
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>interface
config>service>vprn>network-interface
config>service>vprn>video-interface

Description Use this command to apply a specific CPU protection policy to the associated interface. For these interface types, the per-source rate limit is not applicable.

If no CPU-protection policy is assigned to an interface, then the default policy is used to limit the overall-rate. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

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

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

none (for video-interfaces, shown as no cpu-protection in CLI)

The configuration of **no cpu-protection** returns the interface to the default policies as shown above.

cpu-protection

Syntax **cpu-protection policy-id** [**mac-monitoring**]

no cpu-protection

Context config>subscriber-mgmt>msap-policy

Description Use this command to apply a specific CPU protection policy to the associated msap-policy. The specified cpu-protection policy will automatically be applied to any MSAPs that are create using the msap-policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

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

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]] |[**ip-src-monitoring**]
no cpu-protection

Context config>service>ies>sub-if>grp-if>sap

Description Use this command to apply a specific CPU protection policy to the associated msap-policy. The specified cpu-protection policy will automatically be applied to any MSAPs that are create using the msap-policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

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

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

ip-src-monitoring — Enables per SAP + IP source address rate limiting for DHCP packets using the per-source-rate from the associated cpu-protection policy.

cpu-protection

Syntax

cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]
no cpu-protection

Context

config>service>epipe>sap
config>service>epipe>spoke-sdp
config>service>ies>interface>sap
config>service>ies>interface>spoke-sdp
config>service>ipipe>sap
config>service>template>vpls-sap-template
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vprn>interface>sap
config>service>vprn>interface>spoke-sdp
config>service>vprn>sub-if>grp-if>sap

Description

Use this command to apply a specific CPU protection policy to the associated SAP, SDP or template. If the mac-monitoring keyword is given then per MAC rate limiting should be performed, using the per-source-rate from the associated cpu-protection policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

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

Default

cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of **no cpu-protection** returns the SAP/SDP/template to the default policies as shown above.

Parameters

mac-monitoring — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

eth-cfm-monitoring — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP/SDP/template.

aggregate — applies the rate limit to the sum of the per-peer packet rates.

car — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.

Show Commands

Security Commands

access-group

Syntax **access-group** [*group-name*]

Context show>system>security

Description This command displays SNMP access group information.

Parameters *group-name* — This command displays information for the specified access group.

Output **Security Access Group Output —** The following table describes security access group output fields..

Table 9: Show System Security Access Group Output Fields

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

Sample Output

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

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

authentication

Syntax **authentication** [**statistics**]

Context show>system>security

Description This command displays system login authentication configuration and statistics.

Parameters **statistics —** Appends login and accounting statistics to the display.

Output **Authentication Output —** The following table describes system security authentication output fields.

Table 10: Show System Security Authentication Output Fields

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

Sample Output

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

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

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

communities

Syntax **communities**

Context show>system>security

Description This command displays SNMP communities.

Output **Communities Output —** The following table describes community output fields.

Table 11: Show Communities Output Fields

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

Sample Output

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

cpm-filter

Syntax **cpm-filter**

Context show>system>security

Description This command displays CPM filters.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description This command displays CPM IP filters.

Parameters **entry** *entry-id* **—** Identifies a CPM filter entry as configured on this system.

Values 1 — 2048

Output **CPM Filter Output —** The following table describes CPM IP filter output fields..

Table 12: Show CPM IP Filter Output Fields

Label	Description
`Entry-Id`	Displays information about the specified management access filter entry
`Dropped`	Displays the number of dropped events.
`Forwarded`	Displays the number of forwarded events.
`Description`	Displays the CPM filter description.
`Log ID`	Displays the log ID where matched packets will be logged.
`Src IP`	Displays the source IP address(/netmask)
`Dest. IP`	Displays the destination IP address(/netmask).
`Src Port`	Displays the source port number (range).
`Dest. Port`	Displays the destination port number (range).
`Protocol`	Displays the Protocol field in the IP header.
`Dscp`	Displays the DSCP field in the IP header.
`Fragment`	Displays the 3-bit fragment flags or 13-bit fragment offset field.
`ICMP Type`	Displays the ICMP type field in the ICMP header.
`ICMP Code`	Displays the ICMP code field in the ICMP header.

Table 12: Show CPM IP Filter Output Fields (Continued)

Label	Description
`TCP-syn`	Displays the SYN flag in the TCP header.
`TCP-ack`	Displays the ACK flag in the TCP header
`Match action`	When the criteria matches, displays drop or forward packet.
`Next Hop`	In case match action is forward, indicates destination of the matched packet.
`Dropped pkts`	Indicates number of matched dropped packets
`Forwarded pkts`	Indicates number of matched forwarded packets.

Sample Output

```
A:ALA-35# show system security cpm-filter ip-filter
===============================================================================
CPM IP Filters
===============================================================================
Entry-Id  Dropped   Forwarded Description
-------------------------------------------------------------------------------
101       25880     0         CPM-Filter 10.4.101.2 #101
102       25880     0         CPM-Filter 10.4.102.2 #102
103       25880     0         CPM-Filter 10.4.103.2 #103
104       25882     0         CPM-Filter 10.4.104.2 #104
105       25926     0         CPM-Filter 10.4.105.2 #105
106       25926     0         CPM-Filter 10.4.106.2 #106
107       25944     0         CPM-Filter 10.4.107.2 #107
108       25950     0         CPM-Filter 10.4.108.2 #108
109       25968     0         CPM-Filter 10.4.109.2 #109
110       25984     0         CPM-Filter 10.4.110.2 #110
111       26000     0         CPM-Filter 10.4.111.2 #111
112       26018     0         CPM-Filter 10.4.112.2 #112
113       26034     0         CPM-Filter 10.4.113.2 #113
114       26050     0         CPM-Filter 10.4.114.2 #114
115       26066     0         CPM-Filter 10.4.115.2 #115
116       26084     0         CPM-Filter 10.4.116.2 #116
===============================================================================
A:ALA-35#

A:ALA-35# show system security cpm-filter ip-filter entry 101
===============================================================================
CPM IP Filter Entry
===============================================================================
Entry Id           : 101
Description : CPM-Filter 10.4.101.2 #101
-------------------------------------------------------------------------------
Filter Entry Match Criteria :
-------------------------------------------------------------------------------
Log Id             : n/a
Src. IP            : 10.4.101.2/32      Src. Port          : 0
Dest. IP           : 10.4.101.1/32      Dest. Port         : 0
Protocol           : 6                  Dscp               : ef
```

```
ICMP Type          : Undefined          ICMP Code          : Undefined
Fragment           : True               Option-present     : Off
IP-Option          : 130/255            Multiple Option    : True
TCP-syn            : Off                TCP-ack            : True
Match action       : Drop
===============================================================================
A:ALA-35#
```

ipv6-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description Displays CPM IPv6 filters.

Parameters **entry** *entry-id* **—** Identifies a CPM IPv6 filter entry as configured on this system.

Values 1 — 2048

Output **CPM Filter Output —** The following table describes CPM IPv6 filter output fields..

Table 13: Show CPM IPv6 Filter Output Fields

Label	Description
Entry-Id	Displays information about the specified management access filter entry
Dropped	Displays the number of dropped events.
Forwarded	Displays the number of forwarded events.
Description	Displays the CPM filter description.
Log ID	Log Id where matched packets will be logged.
Src IP	Displays Source IP address(/netmask)
Dest. IP	Displays Destination IP address(/netmask).
Src Port	Displays Source Port Number (range).
Dest. Port	Displays Destination Port Number (range).
next-header	Displays next-header field in the IPv6 header.
Dscp	Displays Traffic Class field in the IPv6 header.
ICMP Type	Displays ICMP type field in the icmp header.
ICMP Code	Displays ICMP code field in the icmp header.
TCP-syn	Displays the SYN flag in the TCP header.
TCP-ack	Displays the ACK flag in the TCP header

Table 13: Show CPM IPv6 Filter Output Fields (Continued)

Label	Description
`Match action`	When criteria matches, displays drop or forward packet.
`Next Hop`	In case match action is forward, indicates destination of the matched packet.
`Dropped pkts`	Indicating number of matched dropped packets
`Forwarded pkts`	Indicating number of matched forwarded packets.

Sample Output

```
A:ALA-35# show system security cpm-filter ipv6-filter
===============================================================================
CPM IPv6 Filters
===============================================================================
Entry-Id Dropped Forwarded Description
-------------------------------------------------------------------------------
101      25880   0         CPM-Filter 11::101:2 #101
102      25880   0         CPM-Filter 11::102:2 #102
103      25880   0         CPM-Filter 11::103:2 #103
104      25880   0         CPM-Filter 11::104:2 #104
105      25880   0         CPM-Filter 11::105:2 #105
106      25880   0         CPM-Filter 11::106:2 #106
107      25880   0         CPM-Filter 11::107:2 #107
108      25880   0         CPM-Filter 11::108:2 #108
109      25880   0         CPM-Filter 11::109:2 #109
===============================================================================
A:ALA-35#
```

```
A:ALA-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
===============================================================================
A:ALA-35#
```

cpm-queue

Syntax **cpm-queue** *queue-id*

Context show>system>security

Description Displays CPM queues.

Parameters *queue-id* — Specifies an integer value that identifies a CPM queue.

Values 0, 33 — 2000

CPM queue Output — The following table describes CPM queue output fields..

Table 14: Show CPM IPv6 Filter Output Fields

Label	Description
`PIR`	Displays the administrative Peak Information Rate (PIR) for the queue.
`CIR`	Displays the amount of bandwidth committed to the queue.
`CBS`	Displays the amount of buffer drawn from the reserved buffer portion of the queue’s buffer pool.
`MBS`	Displays the maximum queue depth to which a queue can grow.

Sample Output

```
A:ALA-35# show system security cpm-queue 1001
===============================================================================
CPM Queue Entry
===============================================================================
Queue Id           : 1001
-------------------------------------------------------------------------------
Queue Parameters :
-------------------------------------------------------------------------------
PIR                : 10000000          CIR                : 1000000
CBS                : 4096              MBS                : 8192
===============================================================================
A:ALA-35#
```

cpu-protection

Syntax **cpu-protection**

Context show>system>security

Description This command enables the context to display CPU protection information.

Sample Output

```
show system security cpu-protection eth-cfm-monitoring
===============================================================================
  SAP's where the protection policy Eth-CFM rate limit is exceeded
  ===============================================================================
  SAP-Id                                        Service-Id    Plcy
  -------------------------------------------------------------------------------
  1/1/1                                         3             100
  -------------------------------------------------------------------------------
  1 SAP('s) found
  ===============================================================================
  ===============================================================================
  SDP's where the protection policy Eth-CFM rate limit is exceeded
  ===============================================================================
  SDP-Id            Service-Id    Plcy
  -------------------------------------------------------------------------------
  1:3               3             100
  -------------------------------------------------------------------------------
  1 SDP('s) found
  ===============================================================================

  show system security cpu-protection eth-cfm-monitoring service-id 3 sap-id 1/1/1
   ===============================================================================
  Flows exceeding the Eth-CFM monitoring rate limit
  ===============================================================================
  Service-Id : 3
  SAP-Id     : 1/1/1
  Plcy       : 100
  -------------------------------------------------------------------------------
  Limit  MAC-Address        Level  OpCode
    First-Time            Last-Time             Violation-Periods
  -------------------------------------------------------------------------------
  0      8c:8c:8c:8c:8c:8c  1      18
    03/21/2009 23:32:29   03/21/2009 23:34:39   4000000019
  61234  8d:8d:8d:8d:8d:8d  2      19
    03/21/2009 23:32:39   03/21/2009 23:34:59   4000000020
  61234  Aggregated         3      20
    03/21/2009 23:32:49   03/21/2009 23:35:19   4000000021
  61234  8f:8f:8f:8f:8f:8f  4      21
    03/21/2009 23:32:59   03/21/2009 23:35:39   4000000022
  61234  90:90:90:90:90:90  5      22
    03/21/2009 23:33:09   03/21/2009 23:35:59   4000000023
  61234  91:91:91:91:91:91  6      23
    03/21/2009 23:33:19   03/21/2009 23:36:19   4000000024
  61234  92:92:92:92:92:92  7      24
    03/21/2009 23:33:29   03/21/2009 23:36:39   4000000025
  max    Aggregated         0      25
    03/21/2009 23:33:39   03/21/2009 23:36:59   4000000026
  0      94:94:94:94:94:94  1      26
    03/21/2009 23:33:49   03/21/2009 23:37:19   4000000027
  -------------------------------------------------------------------------------
  9 flows(s) found
  ===============================================================================

  show system security cpu-protection eth-cfm-monitoring service-id 3 sdp-id 1:3
  ===============================================================================
  Flows exceeding the Eth-CFM monitoring rate limit
  ===============================================================================
  Service-Id : 3
  SDP-Id     : 1:3
  Plcy       : 100
  -------------------------------------------------------------------------------
```

```
Limit  MAC-Address        Level  OpCode
  First-Time            Last-Time             Violation-Periods
-------------------------------------------------------------------------------
0      8c:8c:8c:8c:8c:8c  1      18
  03/21/2009 23:32:29   03/21/2009 23:34:39   3000000019
61234  8d:8d:8d:8d:8d:8d  2      19
  03/21/2009 23:32:39   03/21/2009 23:34:59   3000000020
61234  Aggregated         3      20
  03/21/2009 23:32:49   03/21/2009 23:35:19   3000000021
61234  8f:8f:8f:8f:8f:8f  4      21
  03/21/2009 23:32:59   03/21/2009 23:35:39   3000000022
61234  90:90:90:90:90:90  5      22
  03/21/2009 23:33:09   03/21/2009 23:35:59   3000000023
61234  91:91:91:91:91:91  6      23
  03/21/2009 23:33:19   03/21/2009 23:36:19   3000000024
61234  92:92:92:92:92:92  7      24
  03/21/2009 23:33:29   03/21/2009 23:36:39   3000000025
max    Aggregated         0      25
  03/21/2009 23:33:39   03/21/2009 23:36:59   3000000026
0      94:94:94:94:94:94  1      26
  03/21/2009 23:33:49   03/21/2009 23:37:19   3000000027
-------------------------------------------------------------------------------
9 flow(s) found
===============================================================================


show system security cpu-protection excessive-sources service-id 3 sdp-id 1:3
===============================================================================
Sources exceeding the per-source rate limit
===============================================================================
Service-Id : 3
SDP-Id     : 1:3
Plcy       : 100
Limit      : 65534
-------------------------------------------------------------------------------
MAC-Address       First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
00:00:00:00:00:01 03/22/2009 00:41:59 03/22/2009 01:53:39 3000000043
00:00:00:00:00:02 03/22/2009 00:43:39 03/22/2009 01:56:59 3000000044
00:00:00:00:00:03 03/22/2009 00:45:19 03/22/2009 02:00:19 3000000045
00:00:00:00:00:04 03/22/2009 00:46:59 03/22/2009 02:03:39 3000000046
00:00:00:00:00:05 03/22/2009 00:48:39 03/22/2009 02:06:59 3000000047
-------------------------------------------------------------------------------
5 source(s) found
===============================================================================


show system security cpu-protection violators sdp
===============================================================================
SDP's where the protection policy overall rate limit is violated
===============================================================================
SDP-Id           Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1:1              3
  100  61234 05/01/2010 01:43:53 06/27/2010 22:37:20 3000000007
1:2              3
  255  max   05/01/2010 01:43:55 06/27/2010 22:37:23 3000000008
1:3              3
```

```
  100  61234 05/01/2010 01:43:57 06/27/2010 22:37:26 3000000009
1:4              3
  255  max   05/01/2010 01:43:59 06/27/2010 22:37:29 3000000010
1:5              3
  100  61234 05/01/2010 01:44:01 06/27/2010 22:37:32 3000000011
-------------------------------------------------------------------------------
5 SDP('s) found
===============================================================================


show system security cpu-protection excessive-sources
===============================================================================
SAP's where the protection policy per-source rate limit is exceeded
===============================================================================
SAP-Id                                       Service-Id
  Plcy Limit
-------------------------------------------------------------------------------
1/1/1                                        3
  100  65534
-------------------------------------------------------------------------------
1 SAP('s) found
===============================================================================
SDP's where the protection policy per-source rate limit is exceeded
===============================================================================
SDP-Id            Service-Id    Plcy    Limit
-------------------------------------------------------------------------------
1:3               3             100     65534
1:4               3             255     max
1:5               3             100     65534
-------------------------------------------------------------------------------
3 SDP('s) found
===============================================================================


show system security cpu-protection policy association
===============================================================================
Associations for CPU Protection policy 100
===============================================================================
Description : (Not Specified)

SAP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SAP 1/1/1                                         mac-monitoring
  SAP 1/1/2                                         eth-cfm-monitoring aggr car
  SAP 1/1/3                                         eth-cfm-monitoring
  SAP 1/1/4
-------------------------------------------------------------------------------
Number of SAP's : 4

SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:1                eth-cfm-monitoring aggr car
  SDP 1:3                eth-cfm-monitoring aggr
  SDP 1:5                mac-monitoring
  SDP 17407:4123456789   eth-cfm-monitoring car
-------------------------------------------------------------------------------
Number of SDP's : 4
```

```
Interface associations
-------------------------------------------------------------------------------
  None

Managed SAP associations
-------------------------------------------------------------------------------
  None

Video-Interface associations
-------------------------------------------------------------------------------
  None

===============================================================================
Associations for CPU Protection policy 254
===============================================================================
Description : Default (Modifiable) CPU-Protection Policy assigned to Access
              Interfaces

SAP associations
-------------------------------------------------------------------------------
  None

SDP associations
-------------------------------------------------------------------------------
  None

Interface associations
-------------------------------------------------------------------------------
Router-Name : Base
  ies6If
Router-Name : vprn7
  vprn7If
-------------------------------------------------------------------------------
Number of interfaces : 2

Managed SAP associations
-------------------------------------------------------------------------------
  None

Video-Interface associations
-------------------------------------------------------------------------------
  None

===============================================================================
Associations for CPU Protection policy 255
===============================================================================
Description : Default (Modifiable) CPU-Protection Policy assigned to Network
              Interfaces

SAP associations
-------------------------------------------------------------------------------
  None

SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:2
  SDP 1:4                Eth-cfm-monitoring
```

```
Service Id  : 6                         Type   : IES
  SDP 1:6
Service Id  : 7                         Type   : VPRN
  SDP 1:7
Service Id  : 9                         Type   : Epipe
  SDP 1:9
Service Id  : 300                       Type   : VPLS
  SDP 1:300
-------------------------------------------------------------------------------
Number of SDP's : 6

Interface associations
-------------------------------------------------------------------------------
Router-Name : Base
  system
-------------------------------------------------------------------------------
Number of interfaces : 1

Managed SAP associations
-------------------------------------------------------------------------------
  None

Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================

show system security cpu-protection policy 100 association
===============================================================================
Associations for CPU Protection policy 100
===============================================================================
Description : (Not Specified)

SAP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SAP 1/1/1                                         mac-monitoring
  SAP 1/1/2                                         eth-cfm-monitoring aggr car
  SAP 1/1/3                                         eth-cfm-monitoring
  SAP 1/1/4
-------------------------------------------------------------------------------
Number of SAP's : 4

SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:1                eth-cfm-monitoring aggr car
  SDP 1:3                eth-cfm-monitoring aggr
  SDP 1:5                mac-monitoring
  SDP 17407:4123456789   eth-cfm-monitoring car
-------------------------------------------------------------------------------
Number of SDP's : 4

Interface associations
-------------------------------------------------------------------------------
  None

Managed SAP associations
-------------------------------------------------------------------------------
```

```
  None

Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================
A:bksim130#

show system security cpu-protection violators
 ==============================================================================
Ports where a rate limit is violated
===============================================================================
Port-Id
  Type Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No ports found
===============================================================================

===============================================================================
Interfaces where the protection policy overall rate limit is violated
===============================================================================
Interface-Name                               Router-Name
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No interfaces found
===============================================================================

===============================================================================
SAP's where the protection policy overall rate limit is violated
===============================================================================
SAP-Id                                       Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1/1/1                                        3
  100  61234 05/01/2010 01:43:41 06/27/2010 22:37:02 3000000001
-------------------------------------------------------------------------------
1 SAP('s) found
===============================================================================

===============================================================================
SDP's where the protection policy overall rate limit is violated
===============================================================================
SDP-Id           Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1:1              3
  100  61234 05/01/2010 01:43:41 06/27/2010 22:37:02 3000000001
1:2              3
  255  max   05/01/2010 01:43:43 06/27/2010 22:37:05 3000000002
1:3              3
  100  61234 05/01/2010 01:43:45 06/27/2010 22:37:08 3000000003
1:4              3
  255  max   05/01/2010 01:43:47 06/27/2010 22:37:11 3000000004
1:5              3
  100  61234 05/01/2010 01:43:49 06/27/2010 22:37:14 3000000005
-------------------------------------------------------------------------------
5 SDP('s) found
===============================================================================
===============================================================================
Video clients where the protection policy per-source rate limit is violated
===============================================================================
Client IP Address  Video-Interface                 Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No clients found
===============================================================================
```

excessive-sources

Syntax **excessive-sources** [**service-id** *service-id* **sap-id** *sap-id*]

Context show>system>security>cpu-protection

Description This command displays sources exceeding their per-source rate limit.

Parameters **service-id** *service-id* — Displays information for services exceeding their per-source rate limit.

sap-id *sap-id* **—** Displays information for SAPs exceeding their per-source rate limit.

policy

Syntax **policy** [*policy-id*] **association**

Context show>system>security>cpu-protection

Description This command displays CPU protection policy information.

Parameters *policy-id* — Displays CPU protection policy information for the specified policy ID>

association — This keyword displays policy-id associations.

protocol-protection

Syntax **protocol-protection**

Context show>system>security>cpu-protection

Description This command display all interfaces with non-zero drop counters.

violators

Syntax **violators** [**port**] [**interface**] [**sap**] [**video**]

Context show>system>security>cpu-protection

Description This command displays all interfaces, ports or SAPs with CPU protection policy violators.

Parameters **port —** Displays violators associated with the port.

interface — Displays violators associated with the interface.

sap — Displays violators associated with the SAP.

video — Displays violators associated with the video entity.

mac-filter

Syntax **mac-filter** [**entry** *entry-id*]

Context show>system>security>management-access-filter

Description This command displays management access MAC filters.

Parameters **entry** *entry-id* **—** Displays information about the specified entry.

Values 1 — 9999

Sample Output

```
*B:bksim67# show system security management-access-filter mac-filter
==============================================================================
Mac Management Access Filter
==============================================================================
filter type   : mac
Def. Action   : permit
Admin Status  : enabled (no shutdown)
--------------------------------------------------------------------------------
Entry              : 1                    Action             : deny
FrameType          : ethernet_II          Svc-Id             : Undefined
Src Mac            : Undefined
Dest Mac           : Undefined
Dot1p              : Undefined            Ethertype          : Disabled
DSAP               : Undefined            SSAP               : Undefined
Snap-pid           : Undefined            ESnap-oui-zero     : Undefined
cfm-opcode         : Undefined
Log                : disabled             Matches            : 0
==============================================================================
*B:bksim67#
```

keychain

Syntax **keychain** [*key-chain*] [**detail**]

Context show>system>security

Description This command displays keychain information.

Parameters *key-chain* — Specifies the keychain name to display.

detail — Displays detailed keychain information.

Sample Output

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

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

management-access-filter

Syntax **management-access-filter**

Context show>system>security

Description This commend displays management access filter information for IP and MAC filters.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

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

Description This command displays management-access IP filters.

Parameters *entry-id* — Displays information for the specified entry.

Values 1 — 9999

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

Table 15: Show Management Access Filter Output Fields

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

Table 15: Show Management Access Filter Output Fields (Continued)

Label	Description
Action	The action to take for packets that match this filter entry.

```
*A:Dut-F# show system security management-access-filter ip-filter
==============================================================================
IPv4 Management Access Filter
==============================================================================
filter type:  : ip
Def. Action   : permit
Admin Status  : enabled (no shutdown)
------------------------------------------------------------------------------
Entry         : 1
Src IP        : 192.168.0.0/16
Src interface : undefined
Dest port     : undefined
Protocol      : undefined
Router        : undefined
Action        : none
Log           : disabled
Matches       : 0
==============================================================================
*A:Dut-F#
```

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

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

Description This command displays management-access IPv6 filters.

Parameters *entry-id* — Specifies the IPv6 filter entry ID to display.

Values 1 — 9999

Output

```
*A:Dut-C# show system security management-access-filter ipv6-filter entry 1
==============================================================================
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:Dut-C# s
```

password-options

Syntax **password-options**

Context show>system>security

Description This command displays configured password options.

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

Table 16: Show Management Access Filter Output Fields

Label	Description
Password aging in days	Displays the number of days a user password is valid before the user must change their password.
Number of invalid attempts permitted per login	Displays the number of unsuccessful login attempts allowed for the specified **time**.
Time in minutes per login attempt	Displays the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.
Lockout period (when threshold breached)	Displays the lockout period in minutes where the user is not allowed to login.
Authentication order	Displays the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords.
Configured complexity options	Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the **authentication** section.
Minimum password length	Displays the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and DES-keys configured in the system security section.

Sample Output

```
A:ALA-7# show system security password-options
===============================================================================
Password Options
===============================================================================
Password aging in days                          : none
```

```
Number of invalid attempts permitted per login   : 3
Time in minutes per login attempt                : 5
Lockout period (when threshold breached)         : 10
Authentication order                             : radius tacplus local
Configured complexity options                    :
Minimum password length                          : 6
===============================================================================
A:ALA-7#
```

per-peer-queuing

Syntax **per-peer-queuing**

Context show>system>security

Description This command enables or disables CPM hardware queuing per peer. TTL security only operates when per-peer-queuing is enabled.

Output **Per-Peer-Queuing Output —** The following table describes per-peer-queuing output fields.

Table 17: Show Per-Peer-Queuing Output Fields

Label	Description
`Per Peer Queuing`	Displays the status (enabled or disabled) of CPM hardware queuing per peer.
`Total Num of Queues`	Displays the total number of hardware queues.
`Num of Queues In Use`	Displays the total number of hardware queues in use.

Sample Output

```
A:ALA-48# show system security per-peer-queuing
=================================================
CPM Hardware Queuing
=================================================
Per Peer Queuing        : Enabled
Total Num of Queues     : 8192
Num of Queues In Use    : 2
=================================================
A:ALA-48# configure
```

profile

Syntax **profile** [*profile-name*]

Context show>system>security

Description This command displays user profile information.

If the *profile-name* is not specified, then information for all profiles are displayed.

Parameters **profile-name —** Displays information for the specified user profile.

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

Table 18: Show User Profile Output Fields

Label	Description
`User Profile`	Displays the profile name used to deny or permit user console access to a hierarchical branch or to specific commands.
`Def. action`	`Permit all` — Permits access to all commands. `Deny` — Denies access to all commands. `None` — No action is taken.
`Entry`	The entry ID in a policy or filter table.
`Description`	Displays the text string describing the entry.
`Match Command`	Displays the command or subtree commands in subordinate command levels.
`Action`	`Permit all` — Commands matching the entry command match criteria are permitted. `Deny` — Commands not matching the entry command match criteria are not permitted.
`No. of profiles`	The total number of profiles listed.

Sample Output

```
A:ALA-7# show system security profile administrative
===============================================================================
User Profile
===============================================================================
User Profile : administrative
Def. Action  : permit-all
-------------------------------------------------------------------------------
Entry        : 10
Description  :
Match Command: configure system security
Action       : permit
```

```
-------------------------------------------------------------------------------
Entry        : 20
Description  :
Match Command: show system security
Action       : permit
-------------------------------------------------------------------------------
No. of profiles:
===============================================================================
A:ALA-7#
```

source-address

Syntax **source-address**

Context show>system>security

Description This command displays source-address configured for applications.

Output **Source Address Output —** The following table describes source address output fields.

Table 19: Show Source Address Output Fields

Label	Description
`Application`	Displays the source-address application.

`IP address`
`Interface Name`
	Displays the source address IP address or interface name.

`Oper status`	`Up` — The source address is operationally up. `Down` — The source address is operationally down.

Sample Output

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

ssh

Syntax **ssh**

Context show>system>security

Description This command displays all the SSH sessions as well as the SSH status and fingerprint.

Output **SSH Options Output —** The following table describes SSH output fields .

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

Sample output

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

SSH protocol version 2: Enabled
DSA host key finger print:ab:ed:43:6a:75:90:d3:fc:42:59:17:8a:80:10:41:79
=======================================================
Connection    Encryption    Username
=======================================================
192.168.5.218      3des     admin
-------------------------------------------------------
```

```
Number of SSH sessions : 1
=======================================================
ALA-7#
```

```
A:ALA-49>config>system>security# show system security ssh
SSH is disabled
A:ALA-49>config>system>security#
```

user

Syntax **user** [*user-id*] [**detail**]

Context show>system>security

Description This command displays user registration information.

If no command line options are specified, summary information for all users displays.

Parameters *user-id* — Displays information for the specified user.

Default All users

detail — Displays detailed user information to the summary output.

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

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

Label	Description (Continued)
`Local conf`	`Y` — Password authentication is based on the local password database. `N` — Password authentication is not based on the local password database.
`Home directory`	Specifies the local home directory for the user for both console and FTP access.
`Restricted to home`	`Yes` — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device. `No` — The user is allowed to navigate to a directory higher in the directory tree on the home directory device.
`Login exec file`	Displays the user’s login exec file which executes whenever the user successfully logs in to a console session.

Sample Output

```
A:ALA-7# show system security user
===============================================================================
Users
===============================================================================
user id           need    user permissions  password    attempted failed  local
                  new pwd console ftp snmp  expires     logins    logins  conf
-------------------------------------------------------------------------------

admin             n       y       n   n     never       21        0       y
===============================================================================
A:ALA-7#

A:
ALA-7# show system security user detail
===============================================================================
Users
===============================================================================
user id           need    user permissions  password    attempted failed  local
                  new pwd console ftp snmp  expires     logins    logins  conf
-------------------------------------------------------------------------------

admin             n       y       n   n     never       21        0       y
===============================================================================

===============================================================================
User Configuration Detail
===============================================================================
user id            : admin
-------------------------------------------------------------------------------
console parameters
-------------------------------------------------------------------------------
new pw required    : no                 cannot change pw   : no
home directory     : cf3:\
restricted to home : no
login exec file    :
```

```
profile            : administrative
-------------------------------------------------------------------------------
snmp parameters
===============================================================================
A:ALA-7#
```

view

Syntax **view** [*view-name*] [**detail**]

Context show>system>security

Description This command displays the SNMP MIB views.

Parameters *view-name* — Specify the name of the view to display output. If no view name is specified, the complete list of views displays.

detail — Displays detailed view information.

Output **View Output —** The following table describes show view output fields.

Table 20: Show View Output Fields

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

Sample Output

```
A:ALA-48# show system security view
===============================================================================
Views
===============================================================================
view name         oid tree                              mask             permission
-------------------------------------------------------------------------------
iso               1                                                      included
read1             1.1.1.1                               11111111         included
write1            2.2.2.2                               11111111         included
testview          1                                     11111111         included
testview          1.3.6.1.2                             11111111         excluded
mgmt-view         1.3.6.1.2.1.2                                          included
mgmt-view         1.3.6.1.2.1.4                                          included
mgmt-view         1.3.6.1.2.1.5                                          included
mgmt-view         1.3.6.1.2.1.6                                          included
```

```
mgmt-view         1.3.6.1.2.1.7                                     included
mgmt-view         1.3.6.1.2.1.31                                    included
mgmt-view         1.3.6.1.2.1.77                                    included
mgmt-view         1.3.6.1.4.1.6527.3.1.2.3.7                        included
mgmt-view         1.3.6.1.4.1.6527.3.1.2.3.11                       included
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         1.3.6.1.2.1.15                                    included
vprn-view         1.3.6.1.2.1.23                                    included
vprn-view         1.3.6.1.2.1.31                                    included
vprn-view         1.3.6.1.2.1.68                                    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: 33
===============================================================================
A:ALA-48#
```

Login Control

users

Syntax **users**

Context show

Description Displays console user login and connection information.

Output **Users Output —** The following table describes show users output fields.

Table 21: Show Users Output Fields

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

Sample Console Users Output

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

Clear Commands

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 (#, $, spaces, etc.), the entire string must be enclosed within double quotes

ip-address — Clears the authentication statistics for the specified IP address.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears IP filter statistics.

Parameters **entry** *entry-id* **—** Specifies a particular CPM IP filter entry.

Values 1 — 2048

mac-filter

Syntax **mac-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears MAC filter statistics.

Parameters **entry** *entry-id* **—** Specifies a particular CPM MAC filter entry.

Values 1 — 2048

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears IPv6 filter information.

Parameters **entry** *entry-id* **—** Specifies a particular CPM IPv6 filter entry.

Values 1 — 2048

CPU Protection Commands

cpu-protection

Syntax **cpu-protection**

Context clear

Description This command enables the context to clear CPU protection data.

excessive-sources

Syntax **excessive-sources**

Context clear>cpu-protection

Description This command clears the records of sources exceeding their per-source rate limit.

protocol-protection

Syntax **protocol-protection**

Context clear>cpu-protection

Description This command clears the interface counts of packets dropped by protocol protection.

violators

Syntax **violators** [**port**][**interface**][**sap**]

Context clear>cpu-protection

Description This command clears the rate limit violator record.

Parameters **port —** Clears entries for ports.

interface — Clears entries for interfaces.

sap — Clears entries for SAPs.

cpm-queue

Syntax **cpm-queue** *queue-id*

Context clear

Description This command clears CPM queue information.

Parameters *queue-id* — Specifies the CPM queue ID.

Values 33 — 2000

radius-proxy-server

Syntax **radius-proxy-server** *server-name* **statistics**

Context clear>router

Description This command clears RADIUS proxy server data.

Parameters *server-name* — Specifies the proxy server name.

statistics — Clears statistics for the specified server.

Debug Commands

radius

Syntax **radius** [**detail**] [**hex**]
no radius

Context debug

Description This command enables debugging for RADIUS connections.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed output.

hex — Displays the packet dump in hex format.

SNMP

In This Chapter

This chapter provides information to configure SNMP.

Topics in this chapter include:

SNMP Overview

SNMP Architecture

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

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

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

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

- The manager can get information from the agent.
- The manager can set the value of a MIB object that is controlled by an agent.
- The agent can send traps to notify the manager of significant events that occur on the 7750 SR-Series router.

Management Information Base

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

The SNMP agent provides management information to support a collection of IETF specified MIBs and a number of MIBs defined to manage device parameters and network data unique to Alcatel-Lucent's 7750 SR-Series router.

SNMP Protocol Operations

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

- The manager can get information from the agent.
- The manager can set the value of a MIB object that is controlled by an agent.
- The agent notifies the manager of significant events that occur on the 7750 SR-Series router.

SNMP Versions

The agent supports multiple versions of the SNMP protocol.

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.

  SNMPv1 uses a community string match for authentication.
- The 7750 SR OS implementation uses SNMPv2c, the community-based administrative framework for SNMPv2. SNMPv2c uses a community string match for authentication.
- In SNMP Version 3 (SNMPv3), USM defines the user authentication and encryption features. View Access Control MIB (VACM) defines the user access control features. The SNMP-COMMUNITY-MIB is used to associate SNMPv1/SNMPv2c community strings with SNMPv3 VACM access control.

  SNMPv3 uses a username match for authentication.

Management Information Access Control

By default, the 7750 SR OS implementation of SNMP uses SNMPv3. SNMPv3 incorporates security model and security level features. A security model is the authentication type for the group and the security level is the permitted level of security within a security model. The combination of the security level and security model determines which security mechanism handles an SNMP packet.

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

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

The use of community strings provide minimal security and context checking for both agents and managers that receive requests and initiate trap operations. A community string is a text string that acts like a password to permit access to the agent on the 7750 SR-Series router.

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

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

User-Based Security Model Community Strings

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

Views

Views control the access to a managed object. The total MIB of a 7750 SR-Series router can be viewed as a hierarchical tree. When a view is created, either the entire tree or a portion of the tree can be specified and made available to a user to manage the objects contained in the subtree. Object identifiers (OIDs) uniquely identify managed objects. A view defines the type of operations for the view such as read, write, or notify.

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

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

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

Access Groups

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

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

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

Users

By default, authentication and encryption parameters are not configured. Authentication parameters which a user must use in order to be validated by the 7750 SR device can be modified. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with.

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

Which SNMP Version to Use?

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

To implement SNMPv3, an authentication and encryption method must be assigned to a user in order to be validated by the 7750 SR device. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

Figure 4 depicts the configuration requirements to implement SNMPv1/SNMPv2c, and SNMPv3.

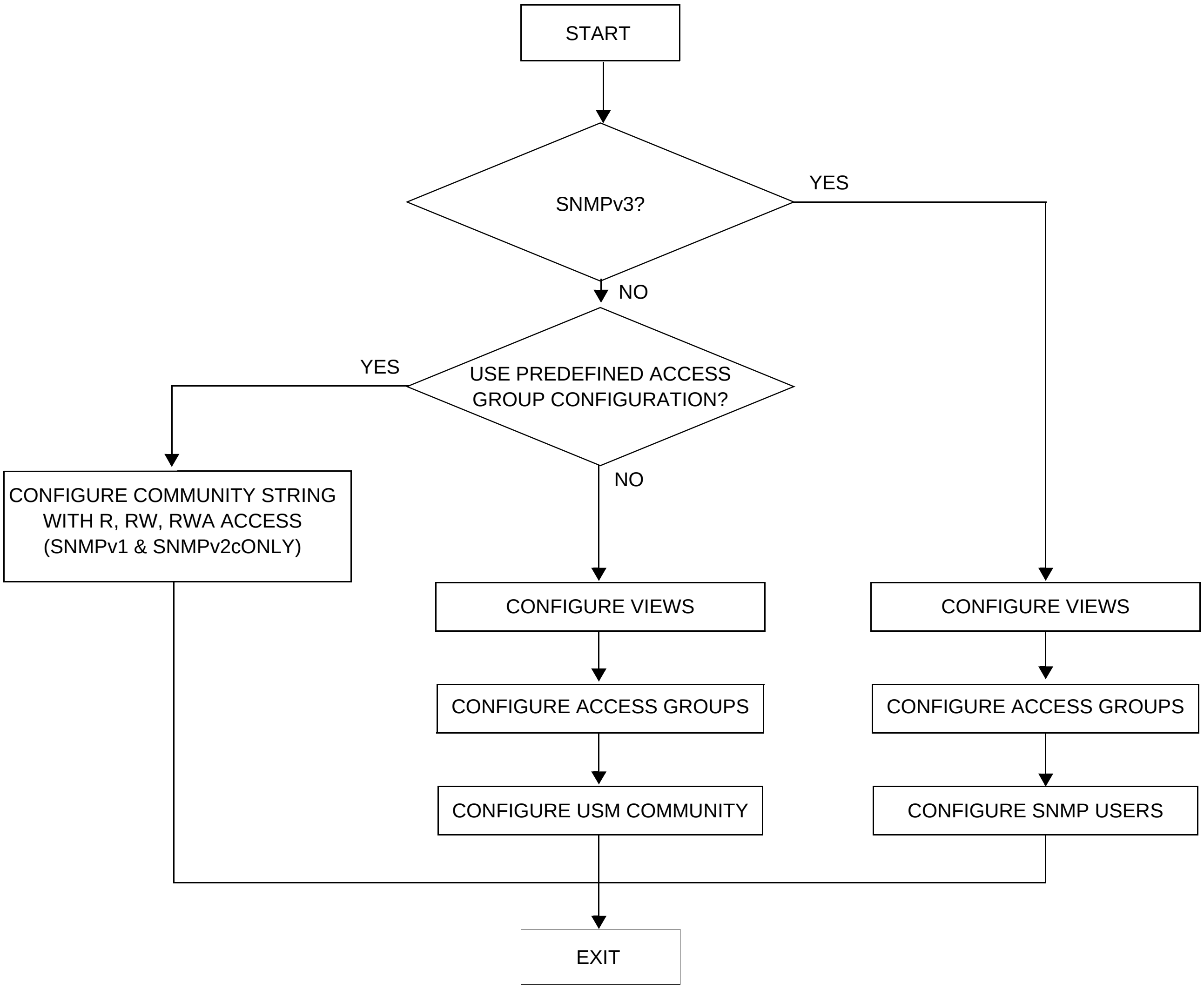

Figure 4: SNMPv1 and SNMPv2c Configuration and Implementation Flow

Configuration Notes

This section describes SNMP configuration caveats.

General

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

  In order to enable SNMP, the portions of the configuration that failed to load must be initialized properly. Start SNMP with the **config>system>snmp>no shutdown** CLI command.
- Use caution when changing the SNMP engine ID. If the SNMP engine ID is changed in the **config>system>snmp> engineID** *engine-id* context, the current configuration must be saved and a reboot must be executed. If not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

- SNMP Configuration Overview on page 262
- Basic SNMP Security Configuration on page 263
- Configuring SNMP Components on page 264

SNMP Configuration Overview

This section describes how to configure SNMP components which apply to SNMPv1 and SNMPv2c, and SNMPv3 on the 7750 SR-Series router.

- Configuring SNMPv1 and SNMPv2c on page 262
- Configuring SNMPv3 on page 262

Configuring SNMPv1 and SNMPv2c

Alcatel-Lucent 7750 SR-Series routers are based on SNMPv3. To use the routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three pre-defined access methods are available when SNMPv1 or SNMPv2c access is required. Each access method (**r**, **rw**, or **rwa**) is associated with an SNMPv3 access group that determines the access privileges and the scope of managed objects available. The **community** command is used to associate a community string with a specific access method and the required SNMP version (SNMPv1 or SNMPv2c). The access methods are:

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

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

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

Configuring SNMPv3

7750 SR OS implements SNMPv3. If security features other than the default views are required, then the following parameters must be configured:

- Configure views
- Configure access groups
- Configure SNMP users

Basic SNMP Security Configuration

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

For SNMPv1 and SNMPv2c:

- Configure community string parameters.

For SNMPv3:

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

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

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

Configuring SNMP Components

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

- Configuring a Community String on page 265
- Configuring View Options on page 266
- Configuring Access Options on page 267
- Configuring USM Community Options on page 269
- Configuring Other SNMP Parameters on page 270

CLI Syntax:

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

Configuring a Community String

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

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

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

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

Use the following CLI syntax to configure community options:

CLI Syntax:

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

The following displays an SNMP community configuration example:

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

Configuring View Options

Use the following CLI syntax to configure view options:

CLI Syntax:

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

The following displays a view configuration example:

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

Configuring Access Options

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

Use the following CLI syntax to configure access features:

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

The following displays an access configuration with the view configurations.

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

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

CLI Syntax:

```
config>system>security# user user-name
   access [ftp] [snmp] [console]
   snmp
      authentication [none]|[[hash]{md5 key|sha key } privacy
      {none|des-key|aes-128-cfb-key key}]
      group group-name
```

The following displays a user’s SNMP configuration example.

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

Configuring USM Community Options

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

By default, the 7750 SR OS implementation of SNMP uses SNMPv3. However, to implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

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

The following displays a SNMP community configuration example:

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

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

Configuring Other SNMP Parameters

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

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

The following example displays the system SNMP default values:

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

SNMP Command Reference

Command Hierarchies

Configuration Commands

SNMP System Commands

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

SNMP Security Commands

```
config
    — system
        — security
            — snmp
                — access group 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 access-permissions [version SNMP-version]
                — no community community-string
                — usm-community community-string group group-name
                — no usm-community community-string
                — view view-name subtree oid-value
                — no view view-name [subtree oid-value]
                    — mask mask-value [type {included | excluded}]
                    — no mask
```

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

```
config
     — system
          — security
               — [no] user user-name
                    — [no] snmp
                         — authentication {[none] | [[hash] {md5 key-1 | sha key-1}
                           privacy {none|des-key|aes-128-cfb-key key-2}]
                         — group group-name
                         — [no] group
```

Show Commands

```
show
     — snmp
          — counters
     — system
          — information
          — security
               — access-group [group-name]
               — authentication [statistics]
               — communities
               — password-options [entry-id]
               — password-options
               — per-peer-queuing
               — profile [profile-name]
               — ssh
               — user [user-id] [detail]
               — view [view-name] [detail]
```

Configuration Commands

SNMP System Commands

engineID

Syntax [**no**] **engineID** *engine-id*

Context config>system>snmp

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

If SNMP engine ID is changed in the **config>system>snmp> engineID** *engine-id* context, the current configuration must be saved and a reboot must be executed. If not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

Note: In conformance with IETF standard RFC 2274, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, hashing algorithms which generate SNMPv3 MD5 or SHA security digest keys use the engineID. Changing the SNMP engineID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable.

When a chassis is replaced, use the engine ID of the first system and configure it in the new system to preserve SNMPv3 security keys. This allows management stations to use their existing authentication keys for the new system.

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

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

Default The engine ID is system generated.

Parameters *engine-id* — An identifier from 10 to 64 hexadecimal digits (5 to 32 octet number), uniquely identifying this SNMPv3 node. This string is used to access this node from a remote host with SNMPv3.

general-port

Syntax **general-port** *port-number*
no general-port

Context config>system>snmp

Description This command configures the port number used by this node to receive SNMP request messages and to send replies. Note that SNMP notifications generated by the agent are sent from the port specified in the **config>log>snmp-trap-group>trap-target** CLI command.

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

Default **161**

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

Values 1 — 65535 (decimal)

packet-size

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

Context config>system>snmp

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

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

Default **1500** bytes

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

Values 484 — 9216

snmp

Syntax **snmp**

Context config>system

Description This command creates the context to configure SNMP parameters.

shutdown

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

Context config>system>snmp

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

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

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

Default **no shutdown**

SNMP Security Commands

access group

Syntax **[no] access group** *group-name* **security-model** *security-model* **security-level** *security-level* [**context** *context-name* [**prefix-match**]] [**read** *view-name-1*] [**write** *view-name-2*] [**notify** *view-name-3*]

Context config>system>security>snmp

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

Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the **community** on page 278).

Default access group configurations cannot be modified or deleted.

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

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

Default **none**

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

security-model {**snmpv1** | **snmpv2c** | **usm**} **—** Specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.

security-level {**no-auth-no-priv** | **auth-no-priv** | **privacy**} **—** Specifies the required authentication and privacy levels to access the views configured in this node.

security-level no-auth-no-privacy — Specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the **none** option.

security-level auth-no-privacy — Specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the **group** and the **user** must be configured for authentication.

security-level privacy — Specifies that both authentication and privacy (encryption) is required. When this option is configured, both the **group** and the user must be configured for **authentication**. The user must also be configured for **privacy**.

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

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

prefix-match — Specifies the context name **prefix-match** keywords, **exact** or **prefix**.

The VPRN context names begin with a **vprn** prefix. The numerical value is associated with the service ID that the VPRN was created with and identifies the service in the service domain. For example, when a new VPRN service is created such as **config>service>vprn 2345 customer 1**, a VPRN with context name **vprn2345** is created.

The **exact** keywork specifies that an exact match between the context name and the prefix value is required. For example, when **context vprn2345 exact** is entered, matches for only **vprn2345** are considered.

The **prefix** keyword specifies that only a match between the prefix and the starting portion of context name is required. If only the **prefix** keyword is specified, simple wildcard processing is used. For example, when **context vprn prefix** is entered, all **vprn** contexts are matched.

Default **exact**

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

Default **none**

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

Values Up to 32 characters

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

Values none

attempts

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

Context config>system>security>snmp

Description This command configures a threshold value of unsuccessful SNMP connection attempts allowed in a specified time frame. The command parameters are used to counter denial of service (DOS) attacks through SNMP.

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

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

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

Default **attempts 20 time 5 lockout 10** — 20 failed SNMP attempts allowed in a 5 minute period with a 10 minute lockout for the host if exceeded.

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

Default **20**

Values 1 — 64

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

Default **5**

Values 0 — 60

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

Default **10**

Values 0 — 1440

community

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

Context config>system>security>snmp

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

When configured, community implies a security model for SNMPv1 and SNMPv2c only.
For SNMPv3 security, the **access group** command on page 276 must be configured.

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

Default **none**

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

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

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

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

Default **both**

mask

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

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

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

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

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

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

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

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

Default none

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

The mask can be entered either:

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

Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.

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

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

Default **included**

snmp

Syntax **snmp**

Context config>system>security

Description This command creates the context to configure SNMPv1, SNMPv2, and SNMPv3 parameters.

usm-community

Syntax **usm-community** *community-string* **group** *group-name*
no usm-community *community-string*

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.

Alcatel-Lucent's SR OS implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (Version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views which specify more specific OIDs (MIB objects in the subtree) can be configured.

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

Default none

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

group — Specify the group that governs the access rights of this community string. This group must be configured first in the **config system security snmp access group** context.
(*Default: none*)

view

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

Context config>system>security>snmp

Description This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.

Once the subtree (OID) is identified, a mask can be created to select the portions of the subtree to be included or excluded for access using this particular view. See the **mask** command. The view(s) configured with this command can subsequently be used in read, write, and notify commands which are used to assign specific access group permissions to created views and assigned to particular access groups.

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

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

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

Default No views are defined.

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

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

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

Show Commands

counters

Syntax **counters**

Context show>snmp

Description This command displays SNMP counters information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.

Output **Counters Output —** The following table describes SNMP counters output fields.

Table 22: Counters Output Fields

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

Sample Output

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

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

information

Syntax **information**

Context show>system

Description This command lists the SNMP configuration and statistics.

Output **System Information Output Fields —** The following table describes system information output fields.

Table 23: Show System Information Output Fields

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

Table 23: Show System Information Output Fields (Continued)

Label	Description
SNMP Index Boot Status	Persistent — Persistent indexes at the last system reboot was enabled. Disabled — Persistent indexes at the last system reboot was disabled.
SNMP Sync State	The state when the synchronization of configuration files between the primary and secondary CPMs finish.
Telnet/SSH/FTP Admin	Displays the administrative state of the Telnet, SSH, and FTP sessions.
Telnet/SSH/FTP Oper	Displays the operational state of the Telnet, SSH, and FTP sessions.
BOF Source	The boot location of the BOF.
Image Source	primary — Specifies whether the image was loaded from the primary location specified in the BOF. secondary — Specifies whether the image was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the image was loaded from the tertiary location specified in the BOF.
Config Source	primary — Specifies whether the configuration was loaded from the primary location specified in the BOF. secondary — Specifies whether the configuration was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the configuration was loaded from the tertiary location specified in the BOF.
Last Booted Config File	Displays the URL and filename of the configuration file used for the most recent boot.
Last Boot Cfg Version	Displays the version of the configuration file used for the most recent boot.
Last Boot Config Header	Displays header information of the configuration file used for the most recent boot.
Last Boot Index Version	Displays the index version used in the most recent boot.
Last Boot Index Header	Displays the header information of the index used in the most recent boot.
Last Saved Config	Displays the filename of the last saved configuration.

Table 23: Show System Information Output Fields (Continued)

Label	Description
Time Last Saved	Displays the time the configuration was most recently saved.
Changes Since Last Save	Yes — The configuration changed since the last save.
	No — The configuration has not changed since the last save.
Time Last Modified	Displays the time of the last modification.
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL — The location and name of the CLI script file executed following successful completion of the boot-up configuration file execution.
	N/A — No CLI script file is executed.
Cfg-OK Script Status	Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-OK Script location.
	Not used — No CLI script file was executed.
Cfg-Fail Script	URL — The location and name of the CLI script file executed following a failed boot-up configuration file execution.
	Not used — No CLI script file was executed.
Cfg-Fail Script Status	Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-Fail Script location.
	Not used — No CLI script file was executed.
Management IP address	The Management IP address of the node.
DNS Server	The DNS address of the node.
DNS Domain	The DNS domain name of the node.
BOF Static Routes	To — The static route destination.
	Next Hop — The next hop IP address used to reach the destination.
	Metric — Displays the priority of this static route versus other static routes.
	None — No static routes are configured.

Sample Output

```
A:ALA-1# show system information
===============================================================================
System Information
===============================================================================
System Name             : ALA-1
System Type             : 7750 SR-12
System Version          : B-0.0.I1204
System Contact          :
System Location         :
System Coordinates      :
System Active Slot      : A
System Up Time          : 1 days, 02:12:57.84 (hr:min:sec)

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

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

BOF Source              : cf1:
Image Source            : primary
Config Source           : primary
Last Booted Config File: ftp://172.22.184.249/./debby-sim1/debby-sim1-config.cfg
Last Boot Cfg Version   : THU FEB 15 16:58:20 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR 7750
                          Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                          reserved. All use subject to applicable license
                          agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                          builder in /rel0.0/I1042/panos/main # Generated THU
                          FEB 11 16:58:20 2007 UTC
Last Boot Index Version: N/A
Last Boot Index Header  : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR 7750
                          Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                          reserved. All use subject to applicable license
                          agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                          builder in /rel0.0/I1042/panos/main # Generated THU
                          FEB 15 16:58:20 2007 UTC
Last Saved Config       : N/A
Time Last Saved         : N/A
Changes Since Last Save: No
Max Cfg/BOF Backup Rev  : 5
Cfg-OK Script           : N/A
Cfg-OK Script Status    : not used
Cfg-Fail Script         : N/A
Cfg-Fail Script Status  : not used

Management IP Addr      : 192.168.2.121/20
DNS Server              : 192.168.1.246
DNS Domain              : eng.timetra.com
BOF Static Routes       :
  To                    Next Hop
  128.251.10.0/23       192.168.1.251
  172.22.184.0/22       192.168.1.251
ATM Location ID         : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ATM OAM Retry Up        : 2
ATM OAM Retry Down      : 4
ATM OAM Loopback Period: 10
===============================================================================
A:ALA-1#
```

access-group

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

Context show>system>security

Description This command displays access-group information.

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

Table 24: Show System Information Output Fields

Label	Description
Group name	The access group name.
Security model	The security model required to access the views configured in this node.
Security level	Specifies the required authentication and privacy levels to access the views configured in this node.
Read view	Specifies the view to read the MIB objects.
Write view	Specifies the view to configure the contents of the agent.
Notify view	Specifies the view to send a trap about MIB objects.
No. of access groups	The total number of configured access groups.

Sample Output

```
A:ALA-1# show system security access-group
===============================================================================
Access Groups
===============================================================================
group name          security  security  read           write          notify
                    model     level     view           view           view
-------------------------------------------------------------------------------
snmp-ro             snmpv1    none      no-security                   no-security
snmp-ro             snmpv2c   none      no-security                   no-security
snmp-rw             snmpv1    none      no-security    no-security    no-security
```

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


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

authentication

Syntax **authentication** [**statistics**]

Context show>system>security

Description This command displays authentication information.

Output **Authentication Output —** The following table describes the authentication output fields.

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

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

Sample Output

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

communities

Syntax **communities**

Context show>system>security

Description This command lists SNMP communities and characterisics.

Output **Communities Ouput —** The following table describes the communities output fields.

Sample Output

Table 25: Show Communities Output Fields

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

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

password-options

Syntax **password-options**

Context show>system>security

Description This command displays password options.

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

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

Sample Output

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

per-peer-queuing

Syntax **per-peer-queuing**

Context show>system>security

Description This command displays displays the number of queues in use by the Qchip, which in turn is used by PPQ, CPM filter, SAP, etc.

Output **Per-Peer_Queuing Output —** The following table describes the per-peer-queuing output fields.

Label	Description
`Per Peer Queuing`	Displays whether per-peer-queuing is enabled or disabled. When enabled, a peering session is established and the router will automatically allocate a separate CPM hardware queue for that peer. When disabled, no hardware queuing per peer occurs.
`Total Num of Queues`	Displays the total number of CPM hardware queues.
`Num of Queues In Use`	Displays the number of CPM hardware queues that are in use.

Sample Output

```
A:ALA-48>show>system>security# per-peer-queuing
=================================================
CPM Hardware Queuing
=================================================
Per Peer Queuing        : Enabled
Total Num of Queues     : 8192
Num of Queues In Use    : 0
=================================================
A:ALA-48>show>system>security#
```

profile

Syntax **profile** [*profile-name*]

Context show>system>security

Description This command displays user profiles for CLI command tree permissions.

Parameters *profile-name* — Specify the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names are listed.

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

Label	Description
`User Profile`	`default` — The action to be given to the user profile if none of the entries match the command. `administrative` — specifies the administrative state for this profile.
`Def. Action`	`none` — No action is given to the user profile when none of the entries match the command. `permit-all` — The action to be taken when an entry matches the command.
`Entry`	`10 - 80` — Each entry represents the configuration for a system user.
`Description`	A text string describing the entry.

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

```
A:ALA-48>config>system>snmp# show system security profile
===============================================================================
User Profile
===============================================================================
User Profile : test
Def. Action  : none
-------------------------------------------------------------------------------
Entry        : 1
Description  :
Match Command:
Action       : unknown
===============================================================================
User Profile : default
Def. Action  : none
-------------------------------------------------------------------------------
Entry        : 10
Description  :
Match Command: exec
Action       : permit
-------------------------------------------------------------------------------
Entry        : 20
Description  :
Match Command: exit
```

```
Action       : permit
-------------------------------------------------------------------------------
Entry        : 30
Description  :
Match Command: help
Action       : permit
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Entry        : 80
Description  :
Match Command: enable-admin
Action       : permit
===============================================================================

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

ssh

Syntax **ssh**

Context show>system>security

Description This command displays all the SSH sessions as well as the SSH status and fingerprint.

Output **SSH Options Output —** The following table describes SSH output fields.

Table 26: Show SSH Output Fields

Label	Description
`SSH status`	`SSH is enabled` — Displays that SSH server is enabled.
	`SSH is disabled` — Displays that SSH server is disabled.
`Key fingerprint`	The key fingerprint is the server’s identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.

Table 26: Show SSH Output Fields (Continued)

Label	Description
`Connection`	The IP address of the connected router(s) (remote client).
`Encryption`	`des` — Data encryption using a private (secret) key. `3des` — An encryption method that allows proprietary information to be transmitted over untrusted networks.
`Username`	The name of the user.
`Number of SSH sessions`	The total number of SSH sessions.

Sample output

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


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

SSH is disabled

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

user

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

Context show>system>security

Description This command displays user information.

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

Table 27: Show User Output Fields

Label	Description
`User ID`	The name of a system user.

Table 27: Show User Output Fields (Continued)

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

Sample Output

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

view

Syntax **view** [*view-name*] [**detail**]

Context show>system>security

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

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

Table 28: Show System Security View Output Fields

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

Sample Output

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

```
A:ALA-1# show system security view no-security detail
===============================================================================
Views
===============================================================================
view name         oid tree                        mask              permission
-------------------------------------------------------------------------------
no-security       1                                                 included
no-security       1.3.6.1.6.3                                       excluded
no-security       1.3.6.1.6.3.10.2.1                                included
```

```
no-security       1.3.6.1.6.3.11.2.1                                included
no-security       1.3.6.1.6.3.15.1.1                                included
-------------------------------------------------------------------------------
No. of Views: 5
===============================================================================
=======================================
no-security used in
=======================================
group name
---------------------------------------
snmp-ro
snmp-rw
=======================================
A:ALA-1#
```

Event and Accounting Logs

In This Chapter

This chapter provides information about configuring event and accounting logs in the 7750 SR.

Topics in this chapter include:

Logging Overview

The two primary types of logging supported in the 7750 SR OS are event logging and accounting logs.

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The 7750 SR groups events into three major categories or event sources:

- Security events — Events that pertain to attempts to breach system security.
- Change events — Events that pertain to the configuration and operation of the node.
- Main events — Events that pertain to applications that are not assigned to other event categories/sources.
- Debug events — Events that pertain to trace or other debugging infomation.

The following are events within the 7750 SR OS and have the following characteristics:

- A time stamp in UTC or local time.
- The generating application.
- A unique event ID within the application.
- The VRF-ID.
- A subject identifying the affected object.
- A short text description.

Event control assigns the severity for each application event and whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7750 SR OS conform to ITU standards M.3100 X.733 & X.21 and are listed in Table 29.

Table 29: Event Severity Levels

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Events that are suppressed by event control will not generate any event log entries. Event control maintains a count of the number of events generated (logged) and dropped (suppressed) for each application event. The severity of an application event can be configured in event control.

An event log within the 7750 SR OS associates the event sources with logging destinations. Examples of logging destinations include, the console session, a specific telnet or SSH session, memory logs, file destinations, SNMP trap groups and syslog destinations. A log filter policy can be associated with the event log to control which events will be logged in the event log based on combinations of application, severity, event ID range, VRF ID, and the subject of the event.

The 7750 SR accounting logs collect comprehensive accounting statistics to support a variety of billing models. The routers collect accounting data on services and network ports on a per-service class basis. In addition to gathering information critical for service billing, accounting records can be analyzed to provide insight about customer service trends for potential service revenue opportunities. Accounting statistics on network ports can be used to track link utilization and network traffic pattern trends. This information is valuable for traffic engineering and capacity planning within the network core.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to customer Service Access Points (SAPs) and network ports. Accounting statistics are collected by counters for individual service queues defined on the customer’s SAP or by the counters within forwarding class (FC) queues defined on the network ports.

The type of record defined within the accounting policy determines where a policy is applied, what statistics are collected and time interval at which to collect statistics.

The only supported destination for an accounting log is a compact flash system device (cf1:or cf2:). Accounting data is stored within a standard directory structure on the device in compressed XML format.

Log Destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. 7750 SR-Series routerssupport the following log destinations:

- Console on page 304
- Session on page 304
- Memory Logs on page 304
- Log Files on page 305
- SNMP Trap Group on page 307
- Syslog on page 307

Only a single log destination can be associated with an event log or with an accounting log. An event log can be associated with multiple event sources, but it can only have a single log destination.

A file destination is the only type of log destination that can be configured for an accounting log.

Console

Sending events to a console destination means the message will be sent to the system console The console device can be used as an event log destination.

Session

A session destination is a temporary log destination which directs entries to the active telnet or SSH session for the duration of the session. When the session is terminated, for example, when the user logs out, the event log is removed. Event logs configured with a session destination are not stored in the configuration file. Event logs can direct log entries to the session destination.

Memory Logs

A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it can hold can be specified, otherwise it will assume a default size. An event log can send entries to a memory log destination.

Log Files

Log files can be used by both event logs and accounting logs and are stored on the compact flash devices (specifically cf1: or cf2:) in the file system. It is recommended that event and accounting logs not be configured on the cf3: device that is used for software images and bootup configuration.

A log file is identified with a single log file ID, but a log file will generally be composed of a number individual files in the file system. A log file is configured with a rollover parameter, expressed in minutes, which represents the length of time an individual log file should be written to before a new file is created for the relevant log file ID. The rollover time is checked only when an update to the log is performed. Thus, complying to this rule is subject to the incoming rate of the data being logged. For example, if the rate is very low, the actual rollover time may be longer than the configured value.

The retention time for a log file specifies the amount of time the file should be retained on the system based on the creation date and time of the file.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file.

Event log files are always created in the **\log** directory on the specified compact flash device. The naming convention for event log files is:

`log` *`eeff-timestamp`*

where:

`ee` is the event log ID

`ff` is the log file destination ID

`timestamp` is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

yyyy is the four-digit year (for example, 2007)

mm is the two digit number representing the month (for example, 12 for December)

dd is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

hh is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

mm is the two digit minute (for example, 30 for 30 minutes past the hour)

ss is the two digit second (for example, 14 for 14 seconds)

Accounting log files are created in the **\act-collect** directory on a compact flash device (specifically *cf1* or *cf2*). The naming convention for accounting log files is nearly the same as for log files except the prefix **act** is used instead of the prefix **log**. The naming convention for accounting logs is:

```
act aaff-timestamp.xml.gz
```

where:

aa is the accounting policy ID

ff is the log file destination ID

timestamp is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

yyyy is the four-digit year (for example, 2007)

mm is the two digit number representing the month (for example, 12 for December)

dd is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

hh is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

mm is the two digit minute (for example, 30 for 30 minutes past the hour)

ss is the two digit second (for example, 14 for 14 seconds)

Accounting logs are `.xml` files created in a compressed format and have a `.gz` extension.

The **\act-collect** directory is where active accounting logs are written. When an accounting log is rolled over, the active file is closed and archived in the **\act** directory before a new active accounting log file created in **\act-collect**.

SNMP Trap Group

An event log can be configured to send events to SNMP trap receivers by specifying an SNMP trap group destination.

An SNMP trap group can have multiple trap targets. Each trap target can have different operational parameters.

A trap destination has the following properties:

- The IP address of the trap receiver.
- The UDP port used to send the SNMP trap.
- SNMP version (v1, v2c, or v3) used to format the SNMP notification.
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

For SNMP traps that will be sent out-of-band through the Management Ethernet port on the SF/CPM, 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 7750 SR.

Each trap target destination of a trap group receives the identical sequence of events as defined by the log ID and the associated sources and log filter applied.

Syslog

An event log can be configured to send events to one syslog destination. Syslog destinations have the following properties:

- Syslog server IP address.
- The UDP port used to send the syslog message.
- The Syslog Facility Code (0 - 23) (default 23 - local 7).
- The Syslog Severity Threshold (0 - 7) - events exceeding the configured level will be sent.

Because syslog uses eight severity levels whereas the 7750 SR-Series uses six internal severity levels, the severity levels are mapped to syslog severities. Table 30 displays the severity level mappings to syslog severities.

Table 30: 7750 SR-Series to Syslog Severity Level Mappings

Severity Level	Numerical Severity (highest to lowest)	Syslog Configured Severity	Definition
	0	emergency	System is unusable
3	1	alert	Action must be taken immediately
4	2	critical	Critical conditions
5	3	error	Error conditions
6	4	warning	Warning conditions
	5	notice	Normal but significant condition
1 cleared 2 indeterminate	6	info	Informational messages
	7	debug	Debug-level messages

Event Logs

Event logs are the means of recording system generated events for later analysis. Events are messages generated by the system by applications or processes within the 7750 SR.

Figure 5 depicts a function block diagram of event logging.

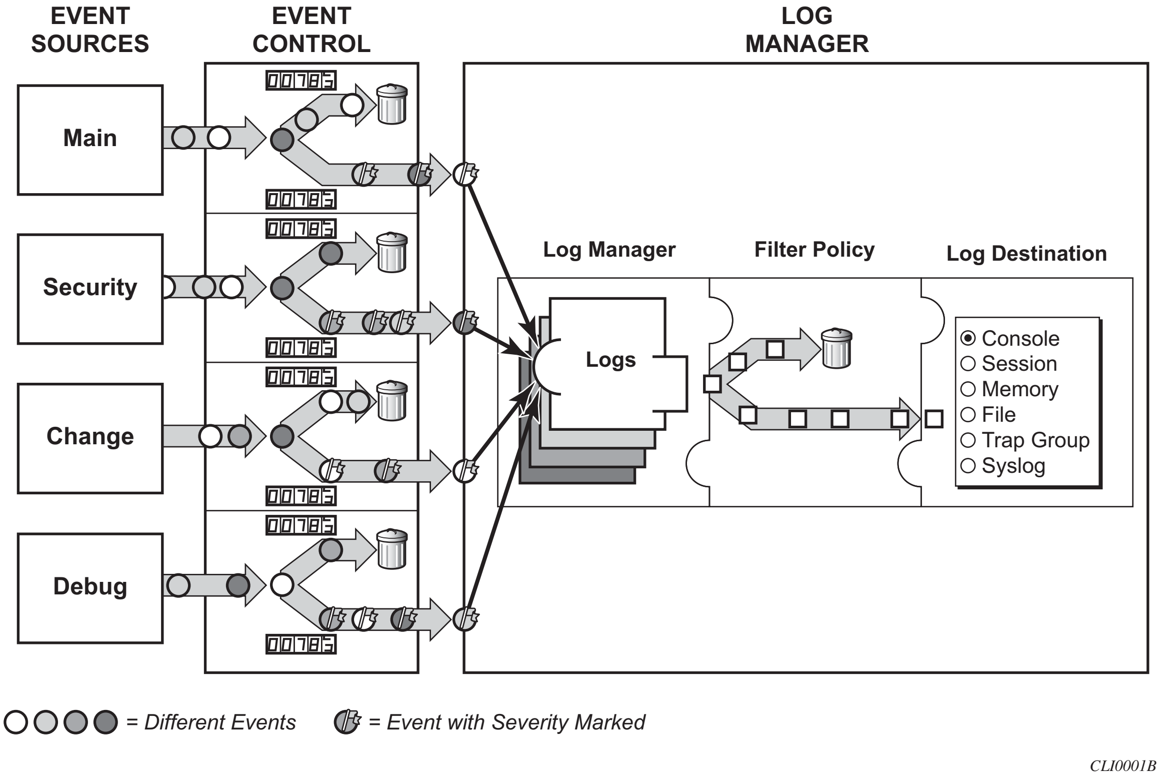

Figure 5: Event Logging Block Diagram

Event Sources

In Figure 5, the event sources are the main categories of events that feed the log manager.

- Security — The security event source is all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the SECURITY application and the authenticationFailure event in the SNMP application.
- Change — The change activity event source is all events that directly affect the configuration or operation of the node. Change events are generated by the USER application.
- 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 7750 SR-Series.

Examples of applications within 7750 SR-Series include IP, MPLS, OSPF, CLI, services, etc. Figure 6 displays an example of the **show log applications** command output which displays all applications.

```
*A:ALA-48# show log applications
==================================
Log Event Application Names
==================================
Application Name
----------------------------------
APS
ATM
BGP
CCAG
CFLOWD
CHASSIS
CPMHWFILTER
DEBUG
DHCP
DOT1X
EFM_OAM
FILTER
GSMP
IGMP
IGMP_SNOOPING
IP
ISIS
LAG
LDP
LOGGER
MCAC
MC_REDUNDANCY
MIRROR
MPLS
MSDP
NTP
OAM
OSPF
PIM
PORT
PPP
QOS
RIP
ROUTE_POLICY
RSVP
SECURITY
SNMP
STP
SUBSCR_MGMT
SVCMGR
SYSTEM
TIP
TOD
USER
VRRP
VRTR
==================================
*A:ALA-48#
```

Figure 6: Show Log Applications Command Output

Event Control

Event control pre-processes the events generated by applications before the event is passed into the main event stream. Event control assigns a severity to application events and can either forward the event to the main event source or suppress the event. Suppressed events are counted in event control, but these events will not generate log entries as it never reaches the log manager.

Simple event throttling is another method of event control and is configured similarly to the generation and suppression options. See Simple Logger Event Throttling on page 318.

Events are assigned a default severity level in the system, but the application event severities can be changed by the user.

Application events contain an event number and description that explains why the event is generated. The event number is unique within an application, but the number can be duplicated in other applications.

The following example, generated by querying event control for application generated events, displays a partial list of event numbers and names.

```
router# show log event-control
=======================================================================
Log Events
=======================================================================
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
-----------------------------------------------------------------------
APS:
   2001 apsEventSwitchover               MI  gen          0           0
   2002 apsEventModeMismatch             MI  gen          0           0
   2003 apsEventChannelMismatch          MI  gen          0           0
,,,
ATM:
   2004 tAtmTcSubLayerDown               MI  gen          0           0
   2005 tAtmTcSubLayerClear              MI  gen          0           0
L  2006 atmVclStatusChange               WA  gen          0           0
...
BGP:
   2001 bgpEstablished                   MI  gen          1           0
   2002 bgpBackwardTransition            WA  gen          7           0
   2003 tBgpMaxPrefix90                  WA  gen          0           0
...
CCAG:
CFLOWD:
   2001 cflowdCreated                    MI  gen          1           0
   2002 cflowdCreateFailure              MA  gen          0           0
   2003 cflowdDeleted                    MI  gen          0           0
...
CHASSIS:
   2001 cardFailure                      MA  gen          0           0
   2002 cardInserted                     MI  gen          4           0
   2003 cardRemoved                      MI  gen          0           0
...
```

```
CPMHWFILTER:
DHCP:
   2001 sdpTlsDHCPSuspiciousPcktRcvd     WA  gen          0           0
   2002 sapTlsDHCPLseStEntriesExceeded   WA  gen          0           0
   2003 sapTlsDHCPLeaseStateOverride     WA  gen          0           0
,,,
DEBUG:
L  2001 traceEvent                       MI  gen          0           0
DOT1X:
FILTER:
   2001 filterPBRPacketsDropped          MI  gen          0           0
IGMP:
   2001 vRtrIgmpIfRxQueryVerMismatch     WA  gen          0           0
   2002 vRtrIgmpIfCModeRxQueryMismatch   WA  gen          0           0
IGMP_SNOOPING:
IP:
L  2001 clearRTMError                    MI  gen          0           0
L  2002 ipEtherBroadcast                 MI  gen          0           0
L  2003 ipDuplicateAddress               MI  gen          0           0
...
ISIS:
   2001 vRtrIsisDatabaseOverload         WA  gen          0           0
```

Log Manager and Event Logs

Events that are forwarded by event control are sent to the log manager. The log manager manages the event logs in the system and the relationships between the log sources, event logs and log destinations, and log filter policies.

An event log has the following properties:

- A unique log ID

  The log ID is a short, numeric identifier for the event log. A maximum of ten logs can be configured at a time.
- One or more log sources

  The source stream or streams to be sent to log destinations can be specified. The source must be identified before the destination can be specified. The events can be from the main event stream, events in the security event stream, or events in the user activity stream.
- One event log destination

  A log can only have a single destination. The destination for the log ID destination can be one of console, session, syslog, snmp-trap-group, memory, or a file on the local file system.
- An optional event filter policy

  An event filter policy defines whether to forward or drop an event or trap-based on match criteria.

Event Filter Policies

The log manager uses event filter policies to allow fine control over which events are forwarded or dropped based on various criteria. Like other policies with the 7750 SR, filter policies have a default action. The default actions are either:

- Forward
- Drop

Filter policies also include a number of filter policy entries that are identified with an entry ID and define specific match criteria and a forward or drop action for the match criteria.

Each entry contains a combination of matching criteria that define the application, event number, router, severity, and subject conditions. The entry’s action determines how the packets should be treated if they have met the match criteria.

Entries are evaluated in order from the lowest to the highest entry ID. The first matching event is subject to the forward or drop action for that entry.

Valid operators are displayed in Table 31:

Table 31: Valid Filter Policy Operators

Operator	Description
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

A match criteria entry can include combinations of:

- Equal to or not equal to a given system application.
- Equal to, not equal to, less than, less than or equal to, greater than or greater than or equal to an event number within the application.
- Equal to, not equal to, less than, less than or equal to, greater than or greater than or equal to a severity level.
- Equal to or not equal to a router name string or regular expression match.
- Equal to or not equal to an event subject string or regular expression match.

Event Log Entries

Log entries that are forwarded to a destination are formatted in a way appropriate for the specific destination whether it be recorded to a file or sent as an SNMP trap, but log event entries have common elements or properties. All application generated events have the following properties:

- A time stamp in UTC or local time.
- The generating application.
- A unique event ID within the application.
- A router name identifying the VRF-ID that generated the event.
- A subject identifying the affected object.
- A short text description.

The general format for an event in an event log with either a memory, console or file destination is as follows.

```
nnnn YYYY/MM/DD HH:MM:SS.SS <severity>:<application> # <event_id> <router-name> <subject>
description
```

The following is an event log example:

```
475 2006/11/27 00:19:40.38 WARNING: SNMP #2007 Base 1/1/1
"interface 1/1/1 came up"
```

The specific elements that compose the general format are described in Table 32.

Table 32: Log Entry Field Descriptions

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

Table 32: Log Entry Field Descriptions (Continued)

Label	Description
`<severity>`	The severity level name of the event. CLEARED — A cleared event (severity number 1). INFO — An indeterminate/informational severity event (severity level 2). CRITICAL — A critical severity event (severity level 3). MAJOR — A major severity event (severity level 4). MINOR — A minor severity event (severity level 5). WARNING — A warning severity event (severity 6).
`<application>`	The application generating the log message.
`<event_id>`	The application’s event ID number for the event.
`<router>`	The router name representing the VRF-ID that generated the event.
`<subject>`	The subject/affected object for the event.
`<description>`	A text description of the event.

Simple Logger Event Throttling

Simple event throttling provides a mechanism to protect event receivers from being overloaded when a scenario causes many events to be generated in a very short period of time. A throttling rate, # events/# seconds, can be configured. Specific event types can be configured to be throttled. Once the throttling event limit is exceeded in a throttling interval, any further events of that type cause the dropped events counter to be incremented. Dropped events counts are displayed by the **show>log>event-control** context. Events are dropped before being sent to one of the logger event collector tasks. There is no record of the details of the dropped events and therefore no way to retrieve event history data lost by this throttling method.

A particular event type can be generated by multiple managed objects within the system. At the point this throttling method is applied the logger application has no information about the managed object that generated the event and cannot distinguish between events generated by object "A" from events generated by object "B". If the events have the same event-id, they are throttled regardless of the managed object that generated them. It also does not know which events may eventually be logged to destination log-id <n> from events that will be logged to destination log-id <m>.

Throttle rate applies commonly to all event types. It is not configurable for a specific event-type.

A timer task checks for events dropped by throttling when the throttle interval expires. If any events have been dropped, a TIMETRA-SYSTEM-MIB::tmnxTrapDropped notification is sent.

Default System Log

Log 99 is a pre-configured memory-based log which logs events from the main event source (not security, debug, etc.). Log 99 exists by default.

The following example displays the log 99 configuration.

```
ALA-1>config>log# info detail
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
...
        snmp-trap-group 7
        exit
...
        log-id 99
            description "Default system log"
            no filter
            from main
            to memory 500
            no shutdown
        exit
----------------------------------------------
ALA-1>config>log#
```

Accounting Logs

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory on compact flash (*cf1:* or *cf2:*) in a compressed (tar) XML format and can be retrieved using FTP or SCP.

A file ID can only be assigned to either one event log ID or one accounting log.

Accounting Records

An accounting policy must define a record name and collection interval. Only one record name can be configured per accounting policy. Also, a record name can only be used in one accounting policy.

The record name, sub-record types, and default collection period for service and network accounting policies are shown below. Table 35, Table 36, and Table 37 provide field descriptions.

Table 33: 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
network-ingress-octets	nio	Network port	15
network-egress-octets	neo	Network port	15
network-egress-packets	nep	Network port	15
network-ingress-packets	nio	Network port	15
compact-service-ingress-octets	ctSio	SAP	5
combined-service-ingress	cmSipo	SAP	5
combined-network-ing-egr-octets	cmNio & cmNeo	Network port	15
combined-service-ing-egr-octets	cmSio & cmSeo	SAP	5
complete-service-ingress-egress	cpSipo & cpSepo	SAP	5
combined-sdp-ingress-egress	cmSdpipo and cmSdpepo	SDP and SDP binding	5
complete-sdp-ingress-egress	cmSdpipo, cmSdpepo, cpSdpipo and cpSdpepo	SDP and SDP binding	5
complete-subscriber-ingress-egress	cpSBipo & cpSBepo	Subscriber profile	5

Table 33: Accounting Record Name and Collection Periods (Continued)

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
aa-protocol	aaProt	AA ISA Group	15
aa-application	aaApp	AA ISA Group	15
aa-app-group	aaAppGrp	AA ISA Group	15
aa-subscriber-protocol	aaSubProt	Special study AA subscriber	15
aa-subscriber-application	aaSubApp	Special study AA subscriber	15
custom-record-aa-sub	aaSubCustom	AA subscriber	15
combined-mpls-lsp-egress	mplsLspEgr	LSP	5
combined-mpls-lsp-ingress	mplsLspIn	LSP	5
saa	saa png trc hop	SAA or SAA test	5

When creating accounting policies, one service accounting policy and one network accounting policy can be defined as default. If statistics collection is enabled on a SAP or network port and no accounting policy is applied, then the respective default policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Each accounting record name is composed of one or more sub-records which is in turn composed of multiple fields. Table 34 lists the accounting policy record names and the statistics that are collected.

Refer to the Application Assurance Statistics Fields Generated per Record table in the 7750 SR-Series OS Integrated Services Adapter Guide for fields names for Application Assurance records.

Table 34: Accounting Record Name Details

Record Name	Sub-Record	Field	Field Description
Service-ingress-octets (sio) (**)	sio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Service-egress-octets (seo) (**)	seo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
Service-ingress-packets (sip) (*) (**)	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) (*) (**)	sep	svc	SvcId
		sap	SapId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
Network-ingress-octets (nio)	nio	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
Network-egress-octets (neo)	neo	port	PortId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Network-ingress-packets (nip)	nip	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
Network Egress Packets (nep)	nep	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
Compact-service-ingress-octets (ctSio)	ctSio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
Combined-service-ingress (cmSipo)	cmSipo	svc	SvcId
		sap	SapId
		qid	QueueId
		hpo	HighPktsOffered
		hpd	HighPktsDropped
		lpo	LowPktsOffered
		lpd	LowPktsDropped
		ucp	UncoloredPacketsOffered
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Combined-network-ing-egr-octets (cmNio & 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
Combined-service-ingr-egr-octets (cmSio & CmSeo)	cmSio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
	cmSeo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Complete-service-ingress-egress (cpSipo & cpSepo)	cpSipo	svc	SvcId
		sap	SapId
		qid	QueueId
		hpo	HighPktsOffered
		hpd	HighPktsDropped
		lpo	LowPktsOffered
		lpd	LowPktsDropped
		ucp	UncoloredPacketsOffered
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		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
Complete-sdp-ingress-egress (cpSdpipo & cpSdpepo)	cpSdpipo	sdp	SdpID
		tpf	TotalPacketsForwarded
		tpd	TotalPacketsDropped
		tof	TotalOctetsForwarded
		tod	TotalOctetsDropped
	cpSdpepo	sdp	SdpID
		tpd	TotalPacketsDropped
		tod	TotalOctetsDropped

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Combined-sdp-ingress-egress (cmSdpipo & cmSdpepo)	cmSdpipo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tpd	TotalPacketsDropped
		tof	TotalOctetsForwarded
		tod	TotalOctetsDropped
	cmSdpepo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
Complete-sdp-ingress-egress (cmSdpipo & cmsdpepo) (cpSdpip & cpSdpepo)	cmSdpipo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tpd	TotalPacketsDropped
		tof	TotalOctetsForwarded
		tod	TotalOctetsDropped
	cmSdpepo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded
	cpSdpipo	sdp	SdpID
		tpf	TotalPacketsForwarded
		tpd	TotalPacketsDropped
		tof	TotalOctetsForwarded
		tod	TotalOctetsDropped
	cpSdpepo	sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) ***	SubscriberInformation	subId	SubscriberId
		subProfile	SubscriberProfile
	Sla-Information****	svc	SvcId
		sap	SapId
		slaProfile	SlaProfile
	cpSBipo	qid	QueueId
		hpo	HighPktsOffered ****
		hpd	HighPktsDropped
		lpo	LowPktsOffered ****
		lpd	LowPktsDropped
		ucp	UncolouredPacketsOffered
		hoo	OfferedHiPrioOctets ****
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered ****
		lod	LowOctetsDropped
		apo	AllPktsOffered ****
		aoo	AllOctetsOffered ****
		uco	UncolouredOctetsOffered
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
	cpSBepo	qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
(continued) Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) ***	cpSBipooc ***	cid	OverrideCounterId
		apo	AllPktsOffered
		hpd	HighPktsDropped
		lpd	LowPktsDropped
		aoo	AllOctetsOffered
		hod	DroppedHiPrioOctets
		lod	LowOctetsDropped
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
		ucp	UncolouredPacketsOffered
		uco	UncolouredOctetsOffered
	cpSBepooc ***	cid	OverrideCounterId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		ofp	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		ipd	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

Table 34: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
		tss	OutTtSumOfSquares
		mni	MinInTt
		mxi	MaxInTt
		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
		ijt	InJitter
		rjt	RtJitter
		prt	ProbeTimeouts
		prf	ProbeFailures
		tat	TraceAddressType
		tav	TraceAddressValue

(*) For a SAP in AAL5 SDU mode, packet counters refer to the number of SDU.

(*) For a SAP in N-to-1 cell mode, packet counters refer to the number of cells.

(**) The number of octets in an ATM sap excludes the Header Error Control (HEC) byte, thus meaning each packet/cell has only 52 bytes instead of the usual 53.

(***) If override counters on the HSMDA are configured (see the 7750 SR Quality of Service Guide).

(****) Not used to identify stats from HSMDA due to MDA architecture. If the statistics are from HSMDA: apo, aoo else lpo/hpo, loo/hoo.

Table 35, Table 36, and Table 37 provide field descriptions.

Table 35: Policer Stats Field Descriptions

Field	Field Description
pid	PolicerId
statmode	PolicerStatMode
aod	AllOctetsDropped
aof	AllOctetsForwarded
aoo	AllOctetsOffered
apd	AllPacketsDropped
apf	AllPacketsForwarded
apo	AllPacketsOffered
hod	HighPriorityOctetsDropped
hof	HighPriorityOctetsForwarded
hoo	HighPriorityOctetsOffered
hpd	HighPriorityPacketsDropped
hpf	HighPriorityPacketsForwarded
hpo	HighPriorityPacketsOffered
iod	InProfileOctetsDropped
iof	InProfileOctetsForwarded
ioo	InProfileOctetsOffered
ipd	InProfilePacketsDropped
ipf	InProfilePacketsForwarded
ipo	InProfilePacketsOffered
lod	LowPriorityOctetsDropped
lof	LowPriorityOctetsForwarded
loo	LowPriorityOctetsOffered
lpd	LowPriorityPacketsDropped
lpf	LowPriorityPacketsForwarded
lpo	LowPriorityPacketsOffered
opd	OutOfProfilePacketsDropped
opf	OutOfProfilePacketsForwarded
opo	OutOfProfilePacketsOffered
ood	OutOfProfileOctetsDropped

Table 35: Policer Stats Field Descriptions (Continued)

Field	Field Description
oof	OutOfProfileOctetsForwarded
ooo	OutOfProfileOctetsOffered
uco	UncoloredOctetsOffered

Table 36: Queue Group Record Types

Record Name	Description
qgone	PortQueueGroupOctetsNetworkEgress
qgosi	PortQueueGroupOctetsServiceIngress
qgose	PortQueueGroupOctetsServiceEgress
qgpne	PortQueueGroupPacketsNetworkEgress
qgpsi	PortQueueGroupPacketsServiceIngress
qgpse	PortQueueGroupPacketsServiceEgress
fpqgosi	ForwardingPlaneQueueGroupOctetsServiceIngress
fpqgoni	ForwardingPlaneQueueGroupOctetsNetworkIngress
fpqgpsi	ForwardingPlaneQueueGroupPacketsServiceIngress
fpqgpni	ForwardingPlaneQueueGroupPacketsNetworkIngress

Table 37: Queue Group Record Type Fields

Field	Field Description
data port	Port (used for port based Queue Groups)
member-port	LAGMemberPort (used for port based Queue Groups)
data slot	Slot (used for Forwarding Plane based Queue Groups)
forwarding-plane	ForwardingPlane (used for Forwarding Plane based Queue Groups)
queue-group	QueueGroupName
instance	QueueGroupInstance
qid	QueueId
pid	PolicerId
statmode	PolicerStatMode
aod...ucp	same as above

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 7750 SR-Series creates two directories on the compact flash to store the files. The following output displays a directory named **act-collect** that holds accounting files that are open and actively collecting statistics. The directory named **act** stores the files that have been closed and are awaiting retrieval.

```
ALA-1>file cf1:\# dir act*
12/19/2006 06:08a      <DIR>          act-collect
12/19/2006 06:08a      <DIR>          act

ALA-1>file cf1:\act-collect\ # dir
Directory of cf1:\act-collect#

12/23/2006 01:46a      <DIR>          .
12/23/2006 12:47a      <DIR>          ..
12/23/2006 01:46a                 112 act1111-20031223-014658.xml.gz
12/23/2006 01:38a                 197 act1212-20031223-013800.xml.gz
```

Accounting files always have the prefix **act** followed by the accounting policy ID, log ID and timestamp. The accounting log file naming and log file destination properties like rollover and retention are discussed in more detail in Log Files on page 305.

Design Considerations

The 7750 SR 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 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. For example, with a 1GB CF and using the default collection interval, the system is expected to hold 48 hours worth of billing information.

Reporting and Time-Based Accounting

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

Overhead Reduction in Accounting: Custom Record

User Configurable Records

Users can define a collection of fields that make up a record. These records can be assigned to an accounting policy. These are user-defined records rather than being limited to pre-defined record types. The operator can select what queues and the counters within these queues that need to be collected. Refer to the predefined records containing a given field for XML field name of a custom record field.

Changed Statistics Only

A record is only generated if a significant change has occurred to the fields being written in a given the record. This capability applies to both ingress and egress records regardless on the method of delivery (such as RADIUS and XML). The capability also applies to Application Assurance records; however without an ability to specify different significant change values and per-field scope (for example, all fields of a custom record are collected if any activity was reported against any of the statistics that are part of the custom record).

Configurable Accounting Records

- XML Accounting Files for Service and ESM-Based Accounting on page 335
- RADIUS Accounting in Networks Using ESM on page 335
- Application Assurance on page 335

XML Accounting Files for Service and ESM-Based Accounting

The custom-record command in the config>log>accounting-policy context provide the flexibility to reduce the volume of data generated, network operators can define the record that needs to be collected. This can eliminate queues or selected counters within these queues that are not relevant for billing.

Record headers including information such as service-ID, SAP-ID, etc., will always be generated.

RADIUS Accounting in Networks Using ESM

The **custom-record** command in the **config>subscr-mgmt>radius-accounting-policy** context provide the flexibility to include individual counters in RADIUS accounting messages. See the CLI tree for commands and syntax.

Application Assurance

An operator can also configure per-AA record type fields of interest to be reported to reduce the volume of statistics and processing times.

Significant Change Only Reporting

Another way to decrease accounting messaging related to overhead is to include only “active” objects in a periodical reporting. An “active object” in this context is an object which has seen a “significant” change in corresponding counters. A significant change is defined in terms of a cumulative value (the sum of all reference counters).

This concept is applicable to all methods used for gathering accounting information, such as an XML file and RADIUS, as well as to all applications using accounting, such as service-acct, ESM-acct, and Application Assurance.

Accounting records are reported at the periodical intervals. This periodic reporting is extended with an internal filter which omits periodical updates for objects whose counter change experienced lower changes than a defined (configurable) threshold.

Specific to RADIUS accounting the **significant-change** command does not affect ACCT-STOP messages. ACCT-STOP messages will be always sent, regardless the amount of change of the corresponding host.

For Application Assurance records, a significant change of 1 in any field of a customized record (send a record if any field changed) is supported. When configured, if any statistic field records activity, an accounting record containing all fields will be collected.

Immediate Completion of Records

Record Completion for XML Accounting

For ESM RADIUS accounting, an accounting stop message is sent when :

- A subscriber/subscriber-host is deleted.
- An SLA profile instance (non-HSMDA) or subscriber instance (HSMDA) is changed.

A similar concept is also used for XML accounting. In case the accounted object is deleted or changed, the latest information will be written in the XML file with a “final” tag indication in the record header.

Configuration Notes

This section describes logging configuration caveats.

- A file or filter cannot be deleted if it has been applied to a log.
- File IDs, syslog IDs, or SNMP trap groups must be configured before they can be applied to a log ID.
- A file ID can only be assigned to *either* one log ID *or* one accounting policy.
- Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.
- The **snmp-trap-id** must be the same as the **log-id**.

Configuring Logging with CLI

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

Topics in this section include:

Log Configuration Overview

Configure logging parameters to save information in a log file or direct the messages to other devices. Logging does the following:

- Provides you with logging information for monitoring and troubleshooting.
- Allows you to select the types of logging information to be recorded.
- Allows you to assign a severity to the log messages.
- Allows you to select the source and target of logging information.

Log Types

Logs can be configured in the following contexts:

- Log file — Log files can contain log event message streams or accounting/billing information. Log file IDs are used to direct events, alarms/traps and debug information to their respective targets.
- SNMP trap groups — SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.
- Syslog — Information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element.
- Event control — Configures a particular event or all events associated with an application to be generated or suppressed.
- Event filters — An event filter defines whether to forward or drop an event or trap based on match criteria.
- Accounting policies — An accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more service access points (SAPs).
- Event logs — An event log defines the types of events to be delivered to its associated destination.
- Event throttling rate — Defines the rate of throttling events.

Basic Event Log Configuration

The most basic log configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays a log configuration example.

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
        event-control "bgp" 2001 generate critical
        file-id 1
            description "This is a test file-id."
            location cf1:
        exit
        file-id 2
            description "This is a test log."
            location cf1:
        exit
        snmp-trap-group 7
            trap-target 11.22.33.44 "snmpv2c" notify-community "public"
        exit
        log-id 2
            from main
            to file 2
        exit
----------------------------------------------
A:ALA-12>config>log#
```

Common Configuration Tasks

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

- Configuring a File ID on page 344
- Configuring an Event Log on page 342
- Configuring an Accounting Policy on page 345
- Configuring Event Control on page 346
- Configuring a Log Filter on page 348
- Configuring an SNMP Trap Group on page 349
- Configuring a Syslog Target on page 357

Configuring an Event Log

A event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

CLI Syntax:

```
config>log
  log-id log-id
     description description-string
     filter filter-id
     from {[main] [security] [change] [debug-trace]}
     to console
     to file file-id
     to memory [size]
     to session
     to snmp [size]
     to syslog syslog-id}
     time-format {local|utc}
     no shutdown
```

The following displays a log file configuration example:

```
ALA-12>config>log>log-id# info
----------------------------------------------
...
     log-id 2
            description "This is a test log file."
            filter 1
            from main security
            to file 1
     exit
...
----------------------------------------------
ALA-12>config>log>log-id#
```

Configuring a File ID

To create a log file a file ID is defined, specifies the target CF drive, and the rollover and retention interval period for the file. The rollover interval is defined in minutes and determines how long a file will be used before it is closed and a new log file is created. The retention interval determines how long the file will be stored on the CF before it is deleted.

Use the following CLI syntax to configure a log file:

CLI Syntax:

```
config>log
 file-id log-file-id
    description description-string
    location cflash-id [backup-cflash-id]
    rollover minutes [retention hours]
```

The following displays a log file configuration example:

```
A:ALA-12>config>log# info
------------------------------------------
        file-id 1
            description "This is a log file."
            location cf1:
            rollover 600 retention 24
        exit
----------------------------------------------
A:ALA-12>config>log#
```

Configuring an Accounting Policy

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory of compact flash (cf1: or cf2:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See Configuring an Event Log on page 342 and Configuring a File ID on page 344.

Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one 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, then the respective default policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Use the following CLI syntax to configure an accounting policy:

CLI Syntax:

```
config>log>
  accounting-policy acct-policy-id interval minutes
     description description-string
     default
     record record-name
     to file log-file-id
     no shutdown
```

The following displays a accounting policy configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
     accounting-policy 4
          description "This is the default accounting policy."
          record complete-service-ingress-egress
          default
          to file 1
     exit
     accounting-policy 5
          description "This is a test accounting policy."
          record service-ingress-packets
          to file 3
     exit
----------------------------------------------
A:ALA-12>config>log#
```

Configuring Event Control

Use the following CLI syntax to configure event control. Note that the **throttle** parameter used in the **event-control** command syntax enables throttling for a specific event type. The **config>log>throttle-rate** command configures the number of events and interval length to be applied to all event types that have throttling enabled by this **event-control** command.

CLI Syntax:

```
config>log
  event-control application-id [event-name|event-number] generate [severity-level] [throttle]
  event-control application-id [event-name|event-number] suppress
  throttle-rate events [interval seconds]
```

The following displays an event control configuration:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        throttle-rate 500 interval 10
        event-control "oam" 2001 generate throttle
        event-control "ospf" 2001 suppress
        event-control "ospf" 2003 generate cleared
        event-control "ospf" 2014 generate critical
..
----------------------------------------------
A:ALA-12>config>log>filter#
```

Configuring Throttle Rate

This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the **event-control** command.

Use the following CLI syntax to configure the throttle rate.

CLI Syntax:

```
config>log#
 throttle-rate events [interval seconds]
```

The following displays a throttle rate configuration example:

```
*A:gal171>config>log# info
---------------------------------------------
        throttle-rate 500 interval 10
        event-control "aps" 2001 generate throttle
----------------------------------------------
*A:gal171>config>log#
```

Configuring a Log Filter

Use the following CLI syntax to configure a log filter:

CLI Syntax:

```
config>log
 filter filter-id
    default-action {drop|forward}
    description description-string
    entry entry-id
       action {drop|forward}
       description description-string
       match
          application {eq|neq} application-id
          number {eq|neq|lt|lte|gt|gte} event-id
          router {eq|neq} router-instance [regexp]
          severity {eq|neq|lt|lte|gt|gte} severity-level
          subject {eq|neq} subject [regexp]
```

The following displays a log filter configuration example:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
        file-id 1
            description "This is our log file."
            location cf1:
            rollover 600 retention 24
        exit
        filter 1
            default-action drop
            description "This is a sample filter."
            entry 1
                action forward
                match
                    application eq "mirror"
                    severity eq critical
                exit
            exit
        exit
...
       log-id 2
            shutdown
            description "This is a test log file."
            filter 1
            from main security
            to file 1
        exit
...
------------------------------------------
A:ALA-12>config>log#
```

Configuring an SNMP Trap Group

The associated *log-id* does not have to configured before a **snmp-trap-group** can be created, however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

Use the following CLI syntax to configure an SNMP trap group:

CLI Syntax:

```
config>log
 snmp-trap-group log-id
    trap-target name [address ip-address] [port port]
          [snmpv1|snmpv2c| snmpv3] notify-community communi-
          tyName |snmpv3SecurityName [security-level {no-
          auth-no-privacy|auth-no-privacy|privacy}] [replay]
```

The following displays a basic SNMP trap group configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
...
      snmp-trap-group 2
         trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
        exit
...
     log-id 2
            description "This is a test log file."
            filter 1
            from main security
            to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays a SNMP trap group, log, and interface configuration examples:

```
A:SetupCLI>config>log# snmp-trap-group 44
A:SetupCLI>config>log>snmp-trap-group# info
----------------------------------------------
            trap-target "xyz-test" address xx.xx.x.x snmpv2c notify-community "xyztesting"
            trap-target "test2" address xx.xx.xx.x snmpv2c notify-community "xyztesting"
----------------------------------------------
*A:SetupCLI>config>log>log-id# info
----------------------------------------------
            from main
            to snmp
----------------------------------------------
*A:SetupCLI>config>router# interface xyz-test
*A:SetupCLI>config>router>if# info
----------------------------------------------
            address xx.xx.xx.x/24
            port 1/1/1
----------------------------------------------
*A:SetupCLI>config>router>if#
```

Setting the Replay Parameter

For this example the replay parameter was set by a SNMP SET request for the trap-target address 10.10.10.3 which is bound to port-id 1/1/1.

```
A:SetupCLI>config>log>snmp-trap-group 44
A:SetupCLI>config>log>snmp-trap-group# info
----------------------------------------------
           trap-target "xyz-test" address 10.10.10.3 snmpv2c notify-community "xyztesting" 
replay
            trap-target "test2" address 20.20.20.5 snmpv2c notify-community "xyztesting"
----------------------------------------------
A:SetupCLI>config>log>snmp-trap-group#
```

In the following output, note that the **Replay** field changed from disabled to enabled.

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : xyz-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : enabled
Replay from : n/a
Last replay : never
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
A:SetupCLI>config>log>snmp-trap-group#
```

Since no events are waiting to be replayed, the log displays as before.

```
A:SetupCLI>config>log>snmp-trap-group# show log log-id 44
===============================================================================
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3819  (wrapped)]

3818 2008/04/22 23:35:39.89 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed admin-
istrative state: inService, operational state: inService"

3817 2008/04/22 23:35:39.89 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"

3816 2008/04/22 23:35:39.89 UTC WARNING: SNMP #2005 Base 1/1/1
"Interface 1/1/1 is operational"

3815 2008/04/22 23:35:39.71 UTC WARNING: SYSTEM #2009 Base CHASSIS
"Status of Mda 1/1 changed administrative state: inService, operational state: inService"

3814 2008/04/22 23:35:38.88 UTC MINOR: CHASSIS #2002 Base Mda 1/2
"Class MDA Module : inserted"

3813 2008/04/22 23:35:38.88 UTC MINOR: CHASSIS #2002 Base Mda 1/1
```

Shutdown In-Band Port

A **shutdown** on the in-band port that the trap-target address is bound to causes the route to that particular trap target to be removed from the route table. When the SNMP module is notified of this event, it marks the trap-target as inaccessible and saves the sequence-id of the first SNMP notification that will be missed by the trap-target.

Example:

```
config>log>snmp-trap-group# exit all
#configure port 1/1/1 shutdown
#
# tools perform log test-event
#
```

The **Replay from** field is updated with the sequence-id of the first event that will be replayed when the trap-target address is added back to the route table.

```
*A:SetupCLI# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : xyz-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : enabled
Replay from : event #3819
Last replay : never
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
*A:SetupCLI#
```

A display of the event log indicates which trap targets are not accessible and waiting for notification replay and the sequence ID of the first notification that will be replayed. Note that if there are more missed events than the log size, the replay will actually start from the first available missed event.

```
*A:SetupCLI# show log log-id 44
===============================================================================
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3821  (wrapped)]
Cannot send to SNMP target address 10.10.10.3.
Waiting to replay starting from event #3819

3820 2008/04/22 23:41:28.00 UTC INDETERMINATE: LOGGER #2011 Base Event Test
"Test event has been generated with system object identifier tmnxModelSR12Reg.
System description: TiMOS-B-0.0.private both/i386 ALCATEL SR 7750 Copyright (c) 2000-2008 
Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Tue Apr 22 14:41:18 PDT 2008 by test123 in /test123/ws/panos/main"

3819 2008/04/22 23:41:20.37 UTC WARNING: MC_REDUNDANCY #2022 Base operational state of peer 
chan*
"The MC-Ring operational state of peer 2.2.2.2 changed to outOfService."

3818 2008/04/22 23:35:39.89 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed admin-
istrative state: inService, operational state: inService"

3823 2008/04/22 23:41:49.82 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"
```

No Shutdown Port

A **no shutdown** command executed on the in-band port to which the trap-target address is bound will cause the route to that trap target to be re-added to the route table. When the SNMP trap module is notified of this event, it resends the notifications that were missed while there was no route to the trap-target address.

Example:

```
configure# port 1/1/1 no shutdown
#
# tools perform log test-event
```

After the notifications have been replayed the **Replay from** field indicates n/a because there are no more notifications waiting to be replayed and the **Last replay** field timestamp has been updated.

```
*A:SetupCLI# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : xyz-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : enabled
Replay from : n/a
Last replay : 04/22/2008 18:52:36
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
*A:SetupCLI#
```

A display of the event log shows that it is no longer waiting to replay notifications to one or more of its trap target addresses. An event message has been written to the logger that indicates the replay to the trap-target address has happened and displays the notification sequence ID of the first and last replayed notifications.

```
*A:SetupCLI# show log log-id 44
===============================================================================
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3827  (wrapped)]

3826 2008/04/22 23:42:02.15 UTC MAJOR: LOGGER #2015 Base Log-id 44
"Missed events 3819 to 3825 from Log-id 44 have been resent to SNMP notification target
address 10.10.10.3."

3825 2008/04/22 23:42:02.15 UTC INDETERMINATE: LOGGER #2011 Base Event Test
"Test event has been generated with system object identifier tmnxModelSR12Reg.
System description: TiMOS-B-0.0.private both/i386 ALCATEL SR 7750 Copyright (c) 2000-2008
Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Tue Apr 22 14:41:18 PDT 2008 by test123 in /test123/ws/panos/main"

3824 2008/04/22 23:41:49.82 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed admin-
istrative s
tate: inService, operational state: inService"

3823 2008/04/22 23:41:49.82 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"
```

Configuring a Syslog Target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

Use the following CLI syntax to configure a syslog file:

CLI Syntax:

```
config>log
  syslog syslog-id
     description description-string
     address ip-address
     log-prefix log-prefix-string
     port port
     level {emergency|alert|critical|error|warning|notice|in-
           fo|debug}
     facility syslog-facility
```

The following displays a syslog configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "This is a syslog file."
            address 10.10.10.104
            facility user
            level warning
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Configuring an Accounting Custom Record

```
A:ALA-48>config>subscr-mgmt>acct-plcy# info
----------------------------------------------
..
            custom-record
                queue 1
                    i-counters
                        high-octets-discarded-count
                        low-octets-discarded-count
                        in-profile-octets-forwarded-count
                        out-profile-octets-forwarded-count
                    exit
                    e-counters
                        in-profile-octets-forwarded-count
                        in-profile-octets-discarded-count
                        out-profile-octets-forwarded-count
                        out-profile-octets-discarded-count
                    exit
                exit
                significant-change 20
                ref-queue all
                    i-counters
                        in-profile-packets-forwarded-count
                        out-profile-packets-forwarded-count
                    exit
                    e-counters
                        in-profile-packets-forwarded-count
                        out-profile-packets-forwarded-count
                    exit
                exit
..
----------------------------------------------
A:ALA-48>config>subscr-mgmt>acct-plcy#
```

Log Management Tasks

This section discusses the following logging tasks:

Modifying a Log File

Use the following CLI syntax to modify a log file:

CLI Syntax:

```
config>log
  log-id log-id
     description description-string
     filter filter-id
     from {[main] [security] [change] [debug-trace]}
     to console
     to file file-id
     to memory [size]
     to session
     to snmp [size]
     to syslog syslog-id}
```

The following displays the current log configuration:

```
ALA-12>config>log>log-id# info
----------------------------------------------
...
    log-id 2
          description "This is a test log file."
          filter 1
          from main security
          to file 1
    exit
...
----------------------------------------------
ALA-12>config>log>log-id#
```

The following displays an example to modify log file parameters:

Example:

```
config# log
config>log# log-id 2
config>log>log-id# description "Chassis log file."
config>log>log-id# filter 2
config>log>log-id# from security
config>log>log-id# exit
```

The following displays the modified log file configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
     log-id 2
            description "Chassis log file."
            filter 2
            from security
            to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, **file 1** is associated with **log-id 2**.

```
A:ALA-12>config>log# info
----------------------------------------------
     file-id 1
             description "LocationTest."
             location cf1:
             rollover 600 retention 24
        exit
...
     log-id 2
             description "Chassis log file."
             filter 2
             from security
             to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Use the following CLI syntax to delete a log file:

CLI Syntax:
```
config>log
  no log-id log-id
      shutdown
```

The following displays an example to delete a log file:

Example:
```
config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

Modifying a File ID

NOTE: When the **file-id** location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear**>**log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log not cleared, the old location remains in effect.

Use the following CLI syntax to modify a log file:

CLI Syntax:

```
config>log
  file-id log-file-id
     description description-string
     location [cflash-id] [backup-cflash-id]
     rollover minutes [retention hours]
```

The following displays the current log configuration:

```
A:ALA-12>config>log# info
------------------------------------------
        file-id 1
            description "This is a log file."
            location cf1:
            rollover 600 retention 24
        exit
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to modify log file parameters:

Example:

```
config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# location cf2:
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file modifications:

```
A:ALA-12>config>log# info
----------------------------------------------
...
       file-id 1
            description "LocationTest."
            location cf2:
            rollover 2880 retention 500
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Deleting a File ID

NOTE: All references to the file ID must be deleted before the file ID can be removed.

Use the following CLI syntax to delete a log ID:

CLI Syntax:
```
config>log
  no file-id log-file-id
```

The following displays an example to delete a file ID:

Example:
```
config>log# no file-id 1
```

Modifying a Syslog ID

NOTE: All references to the syslog ID must be deleted before the syslog ID can be removed.

Use the following CLI syntax to modify a syslog ID parameters:

CLI Syntax:

```
config>log
  syslog syslog-id
     description description-string
     address ip-address
     log-prefix log-prefix-string
     port port
     level {emergency|alert|critical|error|warning|notice|in-
           fo|debug}
     facility syslog-facility
```

The following displays an example of the syslog ID modifications:

Example:

```
config# log
config>log# syslog 1
config>log>syslog$ description "Test syslog."
config>log>syslog# address 10.10.0.91
config>log>syslog# facility mail
config>log>syslog# level info
```

The following displays the syslog configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "Test syslog."
            address 10.10.10.91
            facility mail
            level info
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Deleting a Syslog

Use the following CLI syntax to delete a syslog file:

CLI Syntax:
```
config>log
  no syslog syslog-id
```

The following displays an example to delete a syslog ID:

Example:
```
config# log
config>log# no syslog 1
```

Modifying an SNMP Trap Group

Use the following CLI syntax to modify an SNMP trap group:

CLI Syntax:

```
config>log
  snmp-trap-group log-id
     trap-target name [address ip-address] [port port]
           [snmpv1|snmpv2c| snmpv3] notify-community communi-
           tyName |snmpv3SecurityName [security-level {no-
           auth-no-privacy|auth-no-privacy|privacy}]
```

The following displays the current SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
      snmp-trap-group 10
         trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

Example:

```
config# log
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.10.104:5
config>log>snmp-trap-group# snmp-trap-group# trap-target
10.10.0.91:1 snmpv2c notify-community "com1"
```

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        snmp-trap-group 10
            trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1”
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Deleting an SNMP Trap Group

Use the following CLI syntax to delete a trap target and SNMP trap group:

CLI Syntax:
```
config>log
  no snmp-trap-group log-id
     no trap-target name
```

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
       snmp-trap-group 10
           trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
       exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to delete a trap target and an SNMP trap group.

Example:
```
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.0.91:1
config>log>snmp-trap-group# exit
config>log# no snmp-trap-group 10
```

Modifying a Log Filter

Use the following CLI syntax to modify a log filter:

CLI Syntax:

```
config>log
 filter filter-id
    default-action {drop|forward}
    description description-string
    entry entry-id
       action {drop|forward}
       description description-string
       match
          application {eq|neq} application-id
          number {eq|neq|lt|lte|gt|gte} event-id
          router {eq|neq} router-instance [regexp]
          severity {eq|neq|lt|lte|gt|gte} severity-level
          subject {eq|neq} subject [regexp]
```

The following output displays the current log filter configuration:

```
ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
...
        filter 1
            default-action drop
            description "This is a sample filter."
            entry 1
                action forward
                match
                    application eq "mirror"
                    severity eq critical
                exit
            exit
        exit
...
------------------------------------------
ALA-12>config>log#
```

The following displays an example of the log filter modifications:

Example:

```
config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
A:ALA-12>config>log>filter# info
----------------------------------------
...
        filter 1
            description "This allows <n>."
            entry 1
                action drop
                match
                    application eq "user"
                    number eq 2001
                exit
            exit
        exit
...
----------------------------------------
A:ALA-12>config>log>filter#
```

Deleting a Log Filter

Use the following CLI syntax to delete a log filter:

CLI Syntax: `config>log`
`  no filter` *`filter-id`*

The following output displays the current log filter configuration:

```
A:ALA-12>config>log>filter# info
----------------------------------------
...
        filter 1
            description "This allows <n>."
            entry 1
                action drop
                match
                    application eq "user"
                    number eq 2001
                exit
            exit
        exit
...
----------------------------------------
A:ALA-12>config>log>filter#
```

The following displays an example of the command usage to delete a log filter:

Example: `config>log# no filter 1`

Modifying Event Control Parameters

Use the following CLI syntax to modify event control parameters:

CLI Syntax:

```
config>log
  event-control application-id [event-name|event-number] generate[severity-level] [throttle]
  event-control application-id [event-name|event-number] suppress
```

The following displays the current event control configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
    event-control "bgp" 2014 generate critical
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example of an event control modifications:

Example:

```
config# log
config>log# event-control bgp 2014 suppress
```

The following displays the log filter configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
       event-control "bgp" 2014 suppress
...
----------------------------------------------
A:ALA-12>config>log#
```

Returning to the Default Event Control Configuration

The **no** form of the **event-control** command returns modified values back to the default values.

Use the following CLI syntax to modify event control parameters:

CLI Syntax:
```
config>log
    no event-control application [event-name |event-nunmber]
```

The following displays an example of the command usage to return to the default values:

Example:
```
config# log
config>log# no event-control "bgp" 2001
config>log# no event-control "bgp" 2002
config>log# no event-control "bgp" 2014
```

```
A:ALA-12>config>log# info detail
----------------------------------------------
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        event-control "bgp" 2001 generate minor
        event-control "bgp" 2002 generate warning
        event-control "bgp" 2003 generate warning
        event-control "bgp" 2004 generate critical
        event-control "bgp" 2005 generate warning
        event-control "bgp" 2006 generate warning
        event-control "bgp" 2007 generate warning
        event-control "bgp" 2008 generate warning
        event-control "bgp" 2009 generate warning
        event-control "bgp" 2010 generate warning
        event-control "bgp" 2011 generate warning
        event-control "bgp" 2012 generate warning
        event-control "bgp" 2013 generate warning
        event-control "bgp" 2014 generate warning
        event-control "bgp" 2015 generate critical
        event-control "bgp" 2016 generate warning
...
----------------------------------------------
A:ALA-12>config>log#
```

Log Command Reference

Command Hierarchies

Log Configuration Commands

```
config
    — log
        — event-control application-id [event-name | event-number] [generate [severity-level] [throttle]
        — event-control  application-id [event-name | event-number] suppress
        — no event-control application [event-name | event-number]
        — [no] event-damping
        — route-preference primary {inband | outband} secondary {inband | outband | none}
        — no route-preference
        — throttle-rate events [interval seconds]
        — no throttle-rate
```

Accounting Policy Commands

```
config
    — log
        — collection-interval minutes
        — no collection-interval
        — accounting-policy acct-policy-id
        — no accounting-policy acct-policy-id
            — [no] auto-bandwidth
            — [no] default
            — description description-string
            — no description
            — record record-name
            — no record
            — [no] shutdown
            — to file log-file-id
```

Custom Record Commands

```
config
    — log
            — accounting-policy acct-policy-id [interval minutes]
            — no accounting-policy acct-policy-id
                    — collection-interval minutes
                    — no collection-interval
                    — [no] custom-record
                            — [no] aa-specific
                                    — aa-sub-counters [all]
                                    — no aa-sub-counters
                                            — [no] long-duration-flow-count
                                            — [no] medium-duration-flow-count
                                            — [no] short-duration-flow-count
                                            — [no] total-flow-duration
                                            — [no] total-flows-completed-count
                                    — from-aa-sub-counters [all]
                                    — no from-aa-sub-counters
                                            — [no] flows-active-count[all]
                                            — [no] flows-admitted-count
                                            — [no] flows-denied-count
                                            — [no] max-throughput-octet-count
                                            — [no]  max-throughput-packet-count
                                            — [no]  max-throughput-packet-count
                                            — [no] octets-admitted-count
                                            — [no] octets-denied-count
                                            — [no] packets-admitted-count
                                            — [no] packets-denied-count
                                    — to-aa-sub-counters [all]
                                    — to-aa-sub-counters
                                            — all
                                            — [no] flows-active-count[all]
                                            — [no] flows-admitted-count
                                            — [no] flows-denied-count
                                            — [no] max-throughput-octet-count
                                            — [no]  max-throughput-packet-count
                                            — [no]  max-throughput-packet-count
                                            — [no] octets-admitted-count
                                            — [no] octets-denied-count
                                            — [no] packets-admitted-count
                                            — [no] packets-denied-count
                            — [no] override-counter override-counter-id
                                    — e-counters  [all]
                                    — no e-counters
                                            — [no] in-profile-octets-discarded-count
                                            — [no] in-profile-octets-forwarded-count
                                            — [no] in-profile-packets-discarded-count
                                            — [no] in-profile-packets-forwarded-count
                                            — [no] out-profile-octets-discarded-count
                                            — [no] out-profile-octets-forwarded-count
                                            — [no] out-profile-packets-discarded-count
                                            — [no] out-profile-packets-forwarded-count
                                    — i-counters [all]
```

```
          — no i-counters
                    — [no]  in-profile-octets-discarded-count
                    — [no] in-profile-octets-forwarded-count
                    — [no] in-profile-packets-discarded-count
                    — [no] in-profile-packets-forwarded-count
                    — [no] out-profile-octets-discarded-count
                    — [no] out-profile-octets-forwarded-count
                    — [no] out-profile-packets-discarded-count
                    — [no] out-profile-packets-forwarded-count
— [no] queue queue-id
          — e-counters  [all]
          — no e-counters
                    — [no] in-profile-octets-discarded-count
                    — [no] in-profile-octets-forwarded-count
                    — [no] in-profile-packets-discarded-count
                    — [no] in-profile-packets-forwarded-count
                    — [no] out-profile-octets-discarded-count
                    — [no] out-profile-octets-forwarded-count
                    — [no] out-profile-packets-discarded-count
                    — [no] out-profile-packets-forwarded-count
          — i-counters [all]
          — no i-counters
                    — [no] all-octets-offered-count
                    — [no] all-packets-offered-count
                    — [no] high-octets-discarded-count
                    — [no] high-octets-offered-count
                    — [no] high-packets-discarded-count
                    — [no] high-packets-offered-count
                    — [no] in-profile-octets-forwarded-count
                    — [no] in-profile-packets-forwarded-count
                    — [no] low-octets-discarded-count
                    — [no] low-packets-discarded-count
                    — [no] low-octets-offered-count
                    — [no] low-packets-offered-count
                    — [no] out-profile-octets-forwarded-count
                    — [no] out-profile-packets-forwarded-count
                    — [no] uncoloured-octets-offered-count
                    — [no] uncoloured-packets-offered-count
— ref-aa-specific-counter any
— no ref-aa-specific-counter
— ref-override-counter ref-override-counter-id
— ref-override-counter all
— no ref-override-counter
          — e-counters  [all]
          — no e-counters
                    — [no] in-profile-octets-discarded-count
                    — [no] in-profile-octets-forwarded-count
                    — [no] in-profile-packets-discarded-count
                    — [no] in-profile-packets-forwarded-count
                    — [no] out-profile-octets-discarded-count
                    — [no] out-profile-octets-forwarded-count
                    — [no] out-profile-packets-discarded-count
                    — [no] out-profile-packets-forwarded-count
          — i-counters [all]
          — no i-counters
```

```
                              — [no] all-octets-offered-count
                              — [no] all-packets-offered-count
                              — [no] high-octets-discarded-count
                              — [no] high-octets-offered-count
                              — [no] high-packets-discarded-count
                              — [no] high-packets-offered-count
                              — [no] in-profile-octets-forwarded-count
                              — [no] in-profile-packets-forwarded-count
                              — [no] low-octets-discarded-count
                              — [no] low-packets-discarded-count
                              — [no] low-octets-offered-count
                              — [no] low-packets-offered-count
                              — [no] out-profile-octets-forwarded-count
                              — [no] out-profile-packets-forwarded-count
                              — [no] uncoloured-octets-offered-count
                              — [no] uncoloured-packets-offered-count
              — ref-queue queue-id
              — ref-queue all
              — no ref-queue
                    — e-counters  [all]
                    — no e-counters
                              — [no] in-profile-octets-discarded-count
                              — [no] in-profile-octets-forwarded-count
                              — [no] in-profile-packets-discarded-count
                              — [no] in-profile-packets-forwarded-count
                              — [no] out-profile-octets-discarded-count
                              — [no] out-profile-octets-forwarded-count
                              — [no] out-profile-packets-discarded-count
                              — [no] out-profile-packets-forwarded-count
                    — i-counters [all]
                    — no i-counters
                              — [no] all-octets-offered-count
                              — [no] all-packets-offered-count
                              — [no] high-octets-discarded-count
                              — [no] high-octets-offered-count
                              — [no] high-packets-discarded-count
                              — [no] high-packets-offered-count
                              — [no] in-profile-octets-forwarded-count
                              — [no] in-profile-packets-forwarded-count
                              — [no] low-octets-discarded-count
                              — [no] low-packets-discarded-count
                              — [no] low-octets-offered-count
                              — [no] low-packets-offered-count
                              — [no] out-profile-octets-forwarded-count
                              — [no] out-profile-packets-forwarded-count
              — significant-change delta
              — no significant-change
```

FILE ID COMMANDS

```
config
    — log
          — [no] file-id log-file-id
                — description description-string
                — no description
                — location cflash-id [backup-cflash-id]
```

```
                              — rollover minutes [retention hours]
                              — no rollover
```

EVENT FILTER COMMANDS

```
config
     — log
          — [no] filter filter-id
               — default-action {drop | forward}
               — no default-action
               — description description-string
               — no description
               — [no] entry entry-id
                    — action {drop | forward}
                    — no action
                    — description description-string
                    — no description
                    — [no] match
                         — application {eq | neq} application-id
                         — no application
                         — number {eq | neq | lt | lte | gt | gte} event-id
                         — no number
                         — router {eq | neq} router-instance [regexp]
                         — no router
                         — severity {eq | neq | lt | lte | gt | gte} severity-level
                         — no severity
                         — subject {eq | neq} subject [regexp]
                         — no subject
```

Log ID Commands

```
config
    — log
         — [no] log-id log-id
              — description description-string
              — no description
              — filter filter-id
              — no filter
              — from {[main] [security] [change] [debug-trace]}
              — no from
              — [no] shutdown
              — [no] shutdown
              — time-format {local | utc}
              — to console
              — to file log-file-id
              — to memory [size]
              — to session
              — to snmp [size]
              — to syslog syslog-id
```

SNMP Trap Group Commands

```
config
    — log
         — [no] snmp-trap-group log-id
              — description description-string
              — no description
              — trap-target name [address ip-address] [port port] [snmpv1 | snmpv2c | snmpv3]
                notify-community communityName | snmpv3SecurityName [security-level {no-
                auth-no-privacy | auth-no-privacy | privacy}] [replay]
              — no trap-target name
```

Syslog Commands

```
config
    — log
        — [no] syslog syslog-id
            — address ip-address
            — no address
            — description description-string
            — no description
            — facility syslog-facility
            — no facility
            — level {emergency | alert | critical | error | warning | notice | info | debug}
            — no level
            — log-prefix log-prefix-string
            — no log-prefix
            — port port
            — no port
```

Show Commands

```
show
    — log
        — accounting-policy [acct-policy-id] [access | network]
        — accounting-records
        — applications
        — event-control [application [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]  [subject subject] [ascending | descending]
        — snmp-trap-group [log-id]
        — syslog [syslog-id]
```

Clear Command

```
clear
    — log log-id
```

Configuration Commands

Generic Commands

description

Syntax **description** *string*
no description

Context config>log>filter
config>log>filte>entry
config>log>log-id
config>log>accounting-policy
config>log>file-id
config>log>syslog
config>log>snmp-trap-group

Description This command creates a text description stored in the configuration file for a configuration context. The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

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

Default No text description is associated with this configuration. The string must be entered.

Parameters *string* — The description can contain a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

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

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

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

The **no** form of this command administratively enables an entity.

Default **no shutdown**

Special Cases **log-id** *log-id* — When a *log-id* is shut down, no events are collected for the entity. This leads to the loss of event data.

accounting-policy *accounting Policy* — When an accounting policy is shut down, no accounting data is written to the destination log ID. Counters in the billing data reflect totals, not increments, so when the policy is re-enabled (**no shutdown**) the counters include the data collected during the period the policy was shut down.

Event Control

event-control

Syntax **event-control** *application-id* [*event-name* **|** *event-number*] [**generate** [*severity-level*] [**throttle**]
event-control *application-id* [*event-name* **|** *event-number*] **suppress**
no event-control *application* [*event-name* **|** *event-number*]

Context config>log

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

Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation which directs it to be generated or suppressed.

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

Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are squelched. In reverse, indiscriminate application may cause excessive overhead.

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

The **no** form of the command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, suppress, and throttle options will also be reset to the initial values.

Default Each event has a set of default settings. To display a list of all events and the current configuration use the **event-control** command.

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

Default None, this parameter must be explicitly specified.

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

application_assurance, aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, efm_oam, eth_cfm, filter, gsmp, igmp, igmp_snooping, ip, ipsec, isis, lag, ldp, li, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, msdp, ntp, oam, ospf, pim, pim_snooping, port, ppp, pppoe, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr

event-name | *event-number* — To generate, suppress, or revert to default for a single event, enter the specific number or event short name. If no event number or name is specified, the command applies to all events in the application. To display a list of all event short names use the **event-control** command.

Default none

Values A valid event name or event number.

generate — Specifies that logger event is created when this event occurs. The generate keyword can be used with two optional parameters, *severity-level* and **throttle**.

Default generate

severity-name — An ASCII string representing the severity level to associate with the specified generated events

Default The system assigned severity name

Values One of: cleared, indeterminate, critical, major, minor, warning.

throttle — Specifies whether or not events of this type will be throttled.
By default, event throttling is on for most event types.

suppress — This keyword indicates that the specified events will not be logged. If the **suppress** keyword is not specified then the events are generated by default. For example, **event-control bgp suppress** will suppress all BGP events.

Default generate

event-damping

Syntax [**no**] **event-damping**

Context config>log

Description This command allows the user to set the event damping algorithm to suppress QoS or filter change events.

Note that while this event damping is original behavior for some modules such as service manager, QoS, and filters it can result in the NMS system database being out of sync because of missed change events. On the other hand, if the damping is disabled (**no event-damping**), it may take much longer for a large CLI configuration file to be processed when manually “execed” after system bootup.

route-preference

Syntax **route-preference primary** {**inband | outband**} **secondary** {**inband | outband | none**}
no route-preference

Context config>log

Description This command specifies the primary and secondary routing preference for traffic generated for SNMP notifications and syslog messages. If the remote destination is not reachable through the routing context specified by primary route preference then the secondary routing preference will be attempted.

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

Default no route-preference

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

Default outband

secondary — Specifies the secondary routing preference for traffic generated for SNMP notifications and syslog messages. The routing context specified by the secondary route preference will be attempted if the remote destination was not reachable by the primary routing preference, specified by primary route preference. The value specified for the secondary routing preference must be distinct from the value for primary route preference.

Default inband

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

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

none — Specifies that no attempt will be made to send SNMP notifications and syslog messages to remote destinations.

Log File Commands

file-id

Syntax [**no**] **file-id** *file-id*

Context config>log

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

This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the **to** command under **log-id** or **accounting-policy** to direct specific logging or billing source streams to the file destination.

A file ID can only be assigned to either *one* **log-id** or *one* **accounting-policy**. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.

A file is created when the file ID defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.

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

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

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the file-id
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
  - *yyyy* is the year (for example, 2006)
  - *mm* is the month number (for example, 12 for December)
  - *dd* is the day of the month (for example, 03 for the 3rd of the month)
  - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
  - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
  - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a gz extension.

When initialized, each file will contain:

- The *log-id* description.
- The time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

Default No default file IDs are defined.

Parameters *file-id* — The file identification number for the file, expressed as a decimal integer.

Values 1 — 99

location

Syntax **location** *cflash-id* [*backup-cflash-id*]
no location

Context config>log>file *file-id*

Description This command specifies the primary and optional backup location where the log or billing file will be created.

The **location** command is optional. If the location command not explicitly configured, log files will be created on cf1: and accounting files will be created on cf2: without overflow onto other devices. Generally, cf3: is reserved for system files (configurations, images, etc.).

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 affect until the log is rolled over either because the rollover period has expired or a **clear log** *log-id* command is entered to manually rollover the log file.

When creating files, the primary location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

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

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space does becomes available, then the alarm condition will be cleared.

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

Default Log files are created on cf1: and accounting files are created on cf2:.

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

Values cflash-id: cf1:, cf2:, cf3:

backup-cflash-id — Specify the secondary location.

Values cflash-id: cf1:, cf2:, cf3:

rollover

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

Context config>log>file *file-id*

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

An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the **rollover** time, expressed in minutes.

The **retention** option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.

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

Default **rollover 1440 retention 12**

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

Values 5 — 10080

retention hours. The retention period in hours, expressed as a decimal integer. The retention time is based on the time creation time of the file. The file becomes a candidate for removal once the creation datestamp + rollover time + retention time is less than the current timestamp.

Default 12

Values 1 — 500

Log Filter Commands

filter

Syntax [**no**] **filter** *filter-id*

Context config>log

Description This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.

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

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

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

Default No event filters are defined.

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

Values 1 — 1000

default-action

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

Context config>log>filter *filter-id*

Description The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.

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

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

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

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

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

Log Filter Entry Commands

action

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

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

Description This command specifies a drop or forward action associated with the filter entry. If neither **drop** nor **forward** is specified, the **default-action** will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.

Multiple action statements entered will overwrite previous actions.

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

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

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

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

entry

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

Context config>log>filter *filter-id*

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

Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

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

The **no** form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.

Default No event filter entries are defined. An entry must be explicitly configured.

Parameters *entry-id.* The entry ID uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 — 999

Log Filter Entry Match Commands

match

Syntax [**no**] **match**

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

Description This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.

If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.

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

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

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

Default No match context is defined.

application

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

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

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

An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES etc. Only one application can be specified. The latest **application** command overwrites the previous command.

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

Default **no application** — No application match criterion is specified.

Parameters **eq** | **neq —** The operator specifying the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to

application-id — The application name string.

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, efm_oam, filter, gsmp, igmp, igmp_snooping, ip, isis, lag, ldp, logger, mc_redundancy, mirror, mpls, msdp, ntp, oam, ospf, pim, port, ppp, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr

number

Syntax **number** {**eq | neq | lt | lte | gt | gte**} *event-id*
no number

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

Description This command adds an SR OS application event number as a match criterion.

SR OS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. The latest **number** command overwrites the previous command.

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

Default **no event-number** — No event ID match criterion is specified.

Parameters **eq | neq | lt | lte | gt | gte —** This operator specifies the type of match. Valid operators are listed in the table below. Valid operators are:

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id — The event ID, expressed as a decimal integer.

Values 1 — 4294967295

router

Syntax **router** {**eq | neq**} *router-instance* [**regexp**]
no router

Context config>log>filter>entry>match

Description This command specifies the log event matches for the router.

Parameters **eq —** Determines if the matching criteria should be equal to the specified value.

neq — Determines if the matching criteria should not be equal to the specified value.

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

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** keyword is specified, the string in the **router** command is a regular expression string that will be matched against the subject string in the log event being filtered.

severity

Syntax **severity** {**eq | neq | lt | lte | gt | gte**} *severity-level*
no severity

Context config>log>filter>entry>match

Description This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command.

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

Default **no severity** — No severity level match criterion is specified.

Parameters **eq | neq | lt | lte | gt | gte —** This operator specifies the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

severity-name — The ITU severity level name. The following table lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Values cleared, intermediate, critical, major, minor, warning

subject

Syntax **subject** {**eq|neq**} *subject* [**regexp**]
no subject

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

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

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

Default **no subject —** No subject match criterion specified.

Parameters **eq** | **neq —** This operator specifies the type of match. Valid operators are listed in the following table:

Operator	Notes
eq	equal to
neg	not equal to

subject — A string used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered.

When **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

Syslog Commands

syslog

Syntax [**no**] **syslog** *syslog-id*

Context config>log

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

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

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

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

Default No syslog IDs are defined.

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

Values 1 — 10

address

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

Context config>log>syslog *syslog-id*

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

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

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

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

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

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

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

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

interface: 32 characters maximum, mandatory for link local addressesipv6-addressx:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D
interface: 32 characters maximum, mandatory for link local addresses

facility

Syntax **facility** *syslog-facility*
no facility

Context config>log>syslog *syslog-id*

Description This command configures the facility code for messages sent to the syslog target host.

Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last *facility-code* entered overwrites the previous facility-code.

If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.

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

Default **local7** — syslog entries are sent with the local7 facility code.

Parameters *syslog-facility* — The syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC3164, *The BSD syslog Protocol*, are listed in the table below.

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news
8	uucp

Numerical Code	Facility Code (Continued)
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

Values 0 — 23

log-prefix

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

Context config>log>syslog *syslog-id*

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

RFC3164, *The BSD syslog Protocol,* allows a alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.

Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.

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

Default **no log-prefix** — no prepend log prefix string defined.

Parameters *log-prefix-string* — An alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

level

Syntax **level** *syslog-level*
no level

Context config>log>syslog *syslog-id*

Description This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.

Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.

The **no** form of the command reverts to the default value.

Parameters *value* — The threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

7750 SR severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	0	emergency	system is unusable
3	1	alert	action must be taken immediately
4	2	critical	critical condition
5	3	error	error condition
6	4	warning	warning condition
	5	notice	normal but significant condition
1 cleared 2 indeterminate	6	info	informational messages
	7	debug	debug-level messages

port

Syntax **port** *value*
no port

Context config>log>syslog *syslog-id*

Description This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

The **no** form of the command reverts to default value.

Default **no port**

Parameters *value* — The value is the configured UDP port number used when sending syslog messages.

Values 1 — 65535

throttle-rate

Syntax **throttle-rate** *events* [**interval** *seconds*]
no throttle-rate

Context config>log

Description This command configures an event throttling rate.

Parameters *events* — Specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, for example, the event drop count will be incremented. At the end of the throttle interval if any events have been dropped a trap notification will be sent.

Values 1 — 20000

Default 2000

interval *seconds* — Specifies the number of seconds that an event throttling interval lasts.

Values 1 — 1200

Default 1

SNMP Trap Groups

snmp-trap-group

Syntax [**no**] **snmp-trap-group** *log-id*

Context config>log

Description This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.

A group specifies the types of SNMP traps and specifies the log ID which will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.

To suppress the generation of all alarms and traps see the **event-control** command. To suppress alarms and traps that are sent to this log-id, see the **filter** command. Once alarms and traps are generated they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.

The **no** form of the command deletes the SNMP trap group.

Default There are no default SNMP trap groups.

Parameters *log-id* — The log ID value of a log configured in the **log-id** context. Alarms and traps cannot be sent to the trap receivers until a valid *log-id* exists.

Values 1 — 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**}] [**replay**]
no trap-target *name*

Context config>log>snmp-trap-group

Description This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the **log-id**, **snmp-trap-group** and at least one **trap-target** must be configured.

The **trap-target** command is used to add/remove a trap receiver from an **snmp-trap-group**. The operational parameters specified in the command include:

- The IP address of the trap receiver
- The UDP port used to send the SNMP trap
- SNMP version

- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

A single **snmp-trap-group** *log-id* can have multiple trap-receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.

Note that if the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each7750 SR event log when multiple event logs are directed to the same IP address and port destination.

The **no** form of the command removes the SNMP trap receiver from the SNMP trap group.

Default No SNMP trap targets are defined.

Parameters *name* — Specifies the name of the trap target up to 28 characters in length.

address *ip-address* — The IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group.

Values	ipv4-address	a.b.c.d (host bits must be 0)
	ipv6-address	x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses

port *port* — The destination UDP port used for sending traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address then multiple ports must be configured.

Default 162

Values 1 — 65535

snmpv1 | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Pre-existing conditions are checked before the snmpv3SecurityName is accepted. These are:

- The user name must be configured.
- The v3 access group must be configured.
- The v3 notification view must be configured.

Default snmpv3

Values snmpv1, snmpv2c, snmpv3

notify-community *community* | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If no **notify-community** is configured, then no alarms nor traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community — The community string as required by the **snmpv1** or **snmpv2c** trap receiver. The community string can be an ASCII string up to 31 characters in length.

security-name — The *security-name* as defined in the config>system>security>user context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

security-level {*no-auth-no-privacy* | *auth-no-privacy* | *privacy*} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

Default no-auth-no-privacy. This parameter can only be configured if SNMPv3 is also configured.

Values no-auth-no-privacy, auth-no-privacy, privacy

replay — Enable replay of missed events to target. If replay is applied to an SNMP trap target address, the address is monitored for reachability. Reachability is determined by whether or not there is a route in the routing table by which the target address can be reached. Before sending a trap to a target address, the SNMP module asks the PIP module if there is either an in-band or out-of-band route to the target address. If there is no route to the SNMP target address, the SNMP module saves the sequence-id of the first event that will be missed by the trap target. When the routing table changes again so that there is now a route by which the SNMP target address can be reached, the SNMP module replays (for example, retransmits) all events generated to the SNMP notification log while the target address was removed from the route table.

Note that because of route table change convergence time, it is possible that one or more events may be lost at the beginning or end of a replay sequence.

Logging Destination Commands

filter

Syntax **filter** *filter-id*
no filter

Context config>log>log-id *log-id*

Description This command adds an event filter policy with the log destination.

The **filter** command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination **snmp-trap-group**.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the **filter** command.

Only one filter-id can be configured per log destination.

The **no** form of the command removes the specified event filter from the *log-id*.

Default **no filter** — No event filter policy is specified for a *log-id.*

Parameters *filter-id.* The event filter policy ID is used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in **config>log>filter** *filter-id*.

Values 1 — 1000

from

Syntax **from** {[**main**] [**security**] [**change**] [**debug-trace**]}
no from

Context config>log>log-id *log-id*

Description This command selects the source stream to be sent to a log destination.

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

Only one **from** command may be entered for a single *log-id*. If multiple **from** commands are configured, then the last command entered overwrites the previous **from** command.

The **no** form of the command removes all previously configured source streams.

Default No source stream is configured.

Parameters ***main*** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the **filter** command.

security — Instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the **filter** command.

change — Instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the **filter** command.

debug-trace — Instructs all debug-trace messages in the debug stream to be sent to the destination configured in the **to** command for this destination *log-id*. Filters applied to debug messages are limited to application and subject.

log-id

Syntax [**no**] **log-id** *log-id*

Context config>log

Description This command creates a context to configure destinations for event streams.

The **log-id** context is used to direct events, alarms/traps, and debug information to respective destinations.

A maximum of 10 logs can be configured.

Before an event can be associated with this log-id, the **from** command identifying the source of the event must be configured.

Only one destination can be specified for a *log-id*. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.

Use the **event-control** command to suppress the generation of events, alarms, and traps for all log destinations.

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages.
Log-ID 100 captures log messages with a severity level of major and above.

Note that Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.

The **no** form of the command deletes the log destination ID from the configuration.

Default No log destinations are defined.

Parameters *log-id* — The log ID number, expressed as a decimal integer.

Values 1 — 100

to console

Syntax **to console**

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all the entries are dropped.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

to file

Syntax **to file** *log-file-id*

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a specified file.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

Parameters *log-file-id* — Instructs the events selected for the log ID to be directed to the *log-file-id*. The characteristics of the *log-file-id* referenced here must have already been defined in the **config>log>file** *log-file-id* context.

Values 1 — 99

to memory

Syntax **to memory** [*size*]

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a memory log. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *size* — The *size* parameter indicates the number of events that can be stored in the memory.

Default 100

Values 50 — 1024

to session

Syntax **to session**

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the current console or telnet session. This command is only valid for the duration of the session. When the session is terminated the log ID is removed. A log ID with a *session* destination is not saved in the configuration file.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

to snmp

Syntax **to snmp** [*size*]

Context config>log>log-id *log-id*

Description This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the alarms and traps to be directed to the **snmp-trap-group** associated with *log-id*.

A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the *log-id*.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *size* — The *size* parameter defines the number of events stored in this memory log.

Default 100

Values 50 — 1024

to syslog

Syntax **to syslog** *syslog-id*

Context config>log>log-id

Description This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.

This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1k bytes.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *syslog-id* — Instructs the events selected for the log ID to be directed to the *syslog-id*. The characteristics of the *syslog-id* referenced here must have been defined in the **config>log>syslog** *syslog-id* context.

Values 1 — 10

time-format

Syntax **time-format {local | utc}**

Context config>log>log-id

Description This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default utc

Parameters **local** — Specifies that timestamps are written in the system's local time.

utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Accounting Policy Commands

accounting-policy

Syntax **accounting-policy** *policy-id* [**interval** *minutes*]
no accounting-policy *policy-id*

Context config>log

Description This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.

Access accounting policies are policies that can be applied to one or more SAPs. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.

If an accounting policy is not specified on a SAP, then accounting records are produced in accordance with the access policy designated as the **default**. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.

Only one policy can be regarded as the default access policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new access default policy can be configured.

Network accounting policies are policies that can be applied to one or more network ports or SONET/SDH channels. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports or SONET/SDH channels where this policy is applied.

If no accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy as designated with the **default** command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new network default policy can be configured.

The **no** form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.

Default No default accounting policy is defined.

Parameters *policy-id* — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 — 99

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context config>log>acct-policy

Description This command configures the accounting collection interval.

Parameters *minutes* — Specifies the interval between collections, in minutes.

Values 1 — 120
A range of 1 — 4 is only allowed when the record type is set to SAA.

auto-bandwidth

Syntax [**no**] **auto-bandwidth**

Context config>log>accounting-policy

Description In the configuration of an accounting policy this designates the accounting policy as the one used for auto-bandwidth statistics collection.

Default no auto-bandwidth

default

Syntax [**no**] **default**

Context config>log>accounting-policy

Description This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.

If no access accounting policy is defined on a SAP, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

If no network accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one access accounting policy ID can be designated as the default access policy. Likewise, only one network accounting policy ID can be designated as the default network accounting policy.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of the command removes the default policy designation from the policy ID. The accounting policy will be removed from all SAPs or network ports that do not have this policy explicitly defined.

record

Syntax [**no**] **record** *record-name*

Context config>log>accounting-policy *policy-id*

Description This command adds the accounting record type to the accounting policy to be forwarded to the configured accounting file. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

```
A:ALA-49# 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
9        compact-service-ingress-octets     5
10       combined-service-ingress           5
11       combined-network-ing-egr-octets    15
12       combined-service-ing-egr-octets    5
13       complete-service-ingress-egress    5
14       combined-sdp-ingress-egress        5
15       complete-sdp-ingress-egress        5
16       complete-subscriber-ingress-egress 5
17       aa-protocol                        15
18       aa-application                     15
19       aa-app-group                       15
20       aa-subscriber-protocol             15
21       aa-subscriber-application          15
22       aa-subscriber-app-group            15
23       custom-record-subscriber           5
24       custom-record-service              5
25       custom-record-aa-sub               15
26       queue-group-octets                 15
27       queue-group-packets                15
28       combined-queue-group               15
29       combined-mpls-lsp-ingress          5
30       combined-mpls-lsp-egress           5
31       combined-ldp-lsp-egress            5
32       saa                                5
==========================================================
A:ALA-49#
```

To configure an accounting policy for access ports, select a service record (for example, service-ingress-octets).   To change the record name to another service record then the record command with the new record name can be entered and it will replace the old record name.

When configuring an accounting policy for network ports, a network record should be selected. When changing the record name to another network record, the record command with the new record name can be entered and it will replace the old record name.

If the change required modifies the record from network to service or from service to network, then the old record name must be removed using the **no** form of this command.

Only one record may be configured in a single accounting policy. For example, if an accounting-policy is configured with a **access-egress-octets** record, in order to change it to **service-ingress-octets**, use the **no record** command under the accounting-policy to remove the old record and then enter the **service-ingress-octets** record.

Note that collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of the command removes the record type from the policy.

Default No accounting record is defined

Parameters *record-name* — The accounting record name. The following table lists the accounting record names available and the default collection interval.

Record Type	Accounting Record Name	Default Interval
1	service-ingress-octets	5 minutes
2	service-egress-octets	5 minutes
3	service-ingress-packets	5 minutes
4	service-egress-packets	5 minutes
5	network-ingress-octets	15 minutes
6	network-egress-octets	15 minutes
7	network-ingress-packets	15 minutes
8	network-egress-packets	15 minutes
9	compact-service-ingress-octets	15 minutes
10	combined-service-ingress	5 minutes
11	network-ingr-egr-octets	15 minutes
12	combined-svc-ingr-egr-octets	5 minutes
13	complete-service-ingress-egress	5 minutes
14	complete-sdp-ingress-egress	5 minutes

Record Type	Accounting Record Name	Default Interval (Continued)
15	combined-sdp-ingress-egress	5 minutes
16	complete-subscriber- ingress-egress	5 minutes
17	aa-protocol	15 minutes
18	aa-application	15 minutes
19	aa-application-group	15 minutes
20	aa-subscriber-protocol	15 minutes
21	a-subscriber-application	15 minutes
22	aa-subscriber-application-group	15 minutes
23	custom-record-subscriber	5
24	custom-record-service	5
25	custom-record-aa-sub	15
26	queue-group-octets	15
27	queue-group-packets	15
28	combined-queue-group	15
29	combined-mpls-lsp-ingress	5
30	saa	5
31	combined-mpls-lsp-egress	5
32	combined-ldp-lsp-egress	5

to

Syntax **to file** *file-id*

Context config>log>accounting-policy *policy-id*

This command specifies the destination for the accounting records selected for the accounting policy.

Default No destination is specified.

Parameters *file-id* — The *file-id* option specifies the destination for the accounting records selected for this destination. The characteristics of the file-id must have already been defined in the config>log>file context. A file-id can only be used once.

The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.

If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

Values 1 — 99

Accounting Policy Custom Record Commands

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context config>log>acct-policy

Description This command configures the accounting collection interval.

The **no** form of the command returns the value to the default.

Default 60

Parameters *minutes* — Specifies the collection interval in minutes.

Values 5 — 120

custom-record

Syntax [**no**] **custom-record**

Context config>log>acct-policy

Description This command enables the context to configure the layout and setting for a custom accounting record associated with this accounting policy.

The **no** form of the command reverts the configured values to the defaults.

aa-specific

Syntax [**no**] **aa-specific**

Context config>log>acct-policy>cr

Description This command enables the context to configure information for this custom record.

The **no** form of the command

aa-sub-counters

Syntax **aa-sub-counters** [**all**]
no aa-sub-counters

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure subscriber counter information.

The **no** form of the command

Parameters **all —** Specifies all counters.

long-duration-flow-count

Syntax **long-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the long duration flow count.

The **no** form of the command excludes the long duration flow count in the AA subscriber's custom record.

Default no long-duration-flow-count

medium-duration-flow-count

Syntax [**no**] **medium-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the medium duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the medium duration flow count.

Default no medium-duration-flow-count

short-duration-flow-count

Syntax [**no**] **short-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the short duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the short duration flow count.

Default no short-duration-flow-count

total-flow-duration

Syntax [**no**] **total-flow-duration**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the total flow duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the total flow duration flow count.

total-flows-completed-count

Syntax [**no**] **total-flows-completed-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the total flows completed count in the AA subscriber's custom record.

The **no** form of the command excludes the total flow duration flow count.

from-aa-sub-counters

Syntax [**no**] **from-aa-sub-counters**

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure Application Assurance “from subscriber” counter parameters.

The **no** form of the command excludes the “from subscriber” count.

all

Syntax **all**

Context config>log>acct-policy>cr>aa>aa-to-sub-cntr

Default This command include all counters.

flows-active-count

Syntax [**no**] **flows-active-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the active flow count.

The **no** form of the command excludes the active flow count in the AA subscriber's custom record.

Default no flows-active-count

flows-admitted-count

Syntax [**no**] **flows-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted flow count.

The **no** form of the command excludes the flow’s admitted count in the AA subscriber's custom record.

Default no flows-admitted-count

flows-denied-count

Syntax [**no**] **flows-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the flow’s denied count in the AA subscriber's custom record.

The **no** form of the command excludes the flow’s denied count.

Default no flows-denied-count

max-throughput-octet-count

Syntax [**no**] **max-throughput-octet-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the maximum throughput as measured in the octet count.

The **no** form of the command excludes the maximum throughput octet count.

max-throughput-packet-count

Syntax [**no**] **max-throughput-packet-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the maximum throughput as measured in the packet count.

The **no** form of the command excludes the maximum throughput packet count.

max-throughput-timestamp

Syntax [**no**] **max-throughput-timestamp**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the timestamp of the maximum throughput.

The **no** form of the command excludes the timestamp.

octets-admitted-count

Syntax [**no**] **octets-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted octet count in the AA subscriber's custom record.

The **no** form of the command excludes the admitted octet count.

Default no octets-admitted-count

octets-denied-count

Syntax [**no**] **octets-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the denied octet count in the AA subscriber's custom record.

The **no** form of the command excludes the denied octet count.

Default no octets-denied-count

packets-admitted-count

Syntax [**no**] **packets-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted packet count in the AA subscriber's custom record.

The **no** form of the command excludes the admitted packet count.

Default no packets-admitted-count

packets-denied-count

Syntax [**no**] **packets-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the denied packet count in the AA subscriber's custom record.

The **no** form of the command excludes the denied packet count.

Default no packets-denied-count

to-aa-sub-counters

Syntax **to-aa-sub-counters**
no to-aa-sub-counters

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure Application Assurance “to subscriber” counter parameters.

The **no** form of the command excludes the “to subscriber” count.

override-counter

Syntax [**no**] **override-counter** *override-counter-id*

Context config>log>acct-policy>cr

Description This command enables the context to configure override counter (HSMDA) parameters.

The **no** form of the command removes the ID from the configuration.

Parameters *override-counter-id* — Specifies the override counter ID.

Values 1 — 8

queue

Syntax [**no**] **queue** *queue-id*

Context config>log>acct-policy>cr

Description This command specifies the queue-id for which counters will be collected in this custom record. The counters that will be collected are defined in egress and ingress counters.

The **no** form of the command reverts to the default value.

Parameters *queue-id* — Specifies the queue-id for which counters will be collected in this custom record.

e-counters

Syntax [**no**] **e-counters**

Context config>log>acct-policy>cr>override-cntr
config>log>acct-policy>cr>queue
config>log>acct-policy>cr>ref-override-cntr
config>log>acct-policy>cr>ref-queue

Description This command configures egress counter parameters for this custom record.

The **no** form of the command reverts to the default value.

i-counters

Syntax **i-counters** [**all**]
no i-counters

Context config>log>acct-policy>cr>override-cntr
config>log>acct-policy>cr>ref-override-cntr
config>log>acct-policy>cr>ref-queue

Description This command configures ingress counter parameters for this custom record.

The **no** form of the command

Parameters **all —** Specifies all ingress counters should be included.

in-profile-octets-discarded-count

Syntax [**no**] **in-profile-octets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile octets discarded count.

The **no** form of the command excludes the in-profile octets discarded count.

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile octets forwarded count.

The **no** form of the command excludes the in-profile octets forwarded count.

in-profile-packets-discarded-count

Syntax [**no**] **in-profile-packets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile packets discarded count.

The **no** form of the command excludes the in-profile packets discarded count.

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile packets forwarded count.

The **no** form of the command excludes the in-profile packets forwarded count.

out-profile-octets-discarded-count

Syntax [**no**] **out-profile-octets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets discarded count.

The **no** form of the command excludes the out of profile packets discarded count.

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile octets forwarded count.

The **no** form of the command excludes the out of profile octets forwarded count.

out-profile-packets-discarded-count

Syntax [**no**] **out-profile-packets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets discarded count.

The **no** form of the command excludes the out of profile packets discarded count.

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets forwarded count.

The **no** form of the command excludes the out of profile packets forwarded count.

all-octets-offered-count

Syntax [**no**] **all-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes all octets offered in the count.

The **no** form of the command excludes the octets offered in the count.

Default no all-octets-offered-count

all-packets-offered-count

Syntax [**no**] **all-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes all packets offered in the count.

The **no** form of the command excludes the packets offered in the count.

Default no all-packets-offered-count

high-octets-discarded-count

Syntax [**no**] **high-octets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high octets discarded count.

The **no** form of the command excludes the high octets discarded count.

Default no high-octets-discarded-count

high-octets-offered-count

Syntax [**no**] **high-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high octets offered count.

The **no** form of the command excludes the high octets offered count.

high-packets-discarded-count

Syntax [**no**] **high-packets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high packets discarded count.

The **no** form of the command excludes the high packets discarded count.

Default no high-packets-discarded-count

high-packets-offered-count

Syntax [**no**] **high-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high packets offered count.

The **no** form of the command excludes the high packets offered count.

Default no high-packets-offered -count

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the in profile octets forwarded count.

The **no** form of the command excludes the in profile octets forwarded count.

Default no in-profile-octets-forwarded-count

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the in profile packets forwarded count.

The **no** form of the command excludes the in profile packets forwarded count.

Default no in-profile-packets-forwarded-count

low-octets-discarded-count

Syntax [**no**] **low-octets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low octets discarded count.

The **no** form of the command excludes the low octets discarded count.

Default no low-octets-discarded-count

low-packets-discarded-count

Syntax [**no**] **low-packets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low packets discarded count.

The **no** form of the command excludes the low packets discarded count.

Default no low-packets-discarded-count

low-octets-offered-count

Syntax [**no**] **low-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low octets discarded count.

The **no** form of the command excludes the low octets discarded count.

low-packets-offered-count

Syntax [**no**] **low-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low packets discarded count.

The **no** form of the command excludes the low packets discarded count.

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the out of profile octets forwarded count.

The **no** form of the command excludes the out of profile octets forwarded count.

Default no out-profile-octets-forwarded-count

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the out of profile packets forwarded count.

The **no** form of the command excludes the out of profile packets forwarded count.

Default no out-profile-packets-forwarded-count

uncoloured-octets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the uncoloured octets offered in the count.

The **no** form of the command excludes the uncoloured octets offered in the count.

uncoloured-packets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the uncolored packets offered count.

The **no** form of the command excludes the uncoloured packets offered count.

ref-aa-specific-counter

Syntax **ref-aa-specific-counter any**
no ref-aa-specific-counter

Context config>log>acct-policy>cr

Description This command enables the use of significant-change so only those aa-specific records which have changed in the last accounting interval are written.

The **no** form of the command disables the use of significant-change so all aa-specific records are written whether or not they have changed within the last accounting interval.

Parameters **any —** Indicates that a record is collected as long as any field records activity when non-zero significant-change value is configured.

ref-override-counter

Syntax **ref-override-counter** *ref-override-counter-id*
ref-override-counter all
no ref-override-counter

Context config>log>acct-policy>cr

Description This command configures a reference override counter.

The **no** form of the command reverts to the default value.

Default no ref-override-counter

ref-queue

Syntax **ref-queue** *queue-id*
ref-queue all
no ref-queue

Context config>log>acct-policy>cr

Description This command configures a reference queue.

The **no** form of the command reverts to the default value.

Default no ref-queue

significant-change

Syntax **significant-change** *delta*
no significant-change

Context config>log>acct-policy>cr

Description This command configures the significant change required to generate the record.

Parameters *delta* — Specifies the delta change (significant change) that is required for the custom record to be written to the xml file.

Values 0 — 4294967295 (For custom-record-aa-sub only values 0 or 1 are supported.)

Show Commands

accounting-policy

Syntax **accounting-policy** [*acct-policy-id*] [**access** | **network**]

Context show>log

Description This command displays accounting policy information.

Parameters *policy-id* — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 — 99

access — Only displays access accounting policies.

network — Only displays network accounting policies.

Output **Accounting Policy Output —** The following table describes accounting policy output fields.

Table 38: Show Accounting Policy Output Fields

Label	Description
`Policy ID`	The identifying value assigned to a specific policy.
`Type`	Identifies accounting record type forwarded to the configured accounting file. `access` — Indicates that the policy is an access accounting policy. `network` — Indicates that the policy is a network accounting policy. `none` — Indicates no accounting record types assigned.
`Def`	`Yes` — Indicates that the policy is a default access or network policy. `No` — Indicates that the policy is not a default access or network policy.
`Admin State`	Displays the administrative state of the policy. `Up` — Indicates that the policy is administratively enabled. `Down` — Indicates that the policy is administratively disabled.
`Oper State`	Displays the operational state of the policy. `Up` — Indicates that the policy is operationally up. `Down` — Indicates that the policy is operationally down.

Table 38: Show Accounting Policy Output Fields (Continued)

Label	Description
`Intvl`	Displays the interval, in minutes, in which statistics are collected and written to their destination. The default depends on the record name type.
`File ID`	The log destination.
`Record Name`	The accounting record name which represents the configured record type.
`This policy is applied to`	Specifies the entity where the accounting policy is applied.

Sample Output

```
A:ALA-1# show log accounting-policy
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
10     access  Yes Up    Up    5         3    complete-service-ingress-egress
==============================================================================
A:ALA-1#
```

```
A:ALA-1# show log accounting-policy 10
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 complete-service-ingress-egress

Description : (Not Specified)

This policy is applied to:
    Svc Id: 100  SAP : 1/1/8:0     Collect-Stats
    Svc Id: 101  SAP : 1/1/8:1     Collect-Stats
    Svc Id: 102  SAP : 1/1/8:2     Collect-Stats
    Svc Id: 103  SAP : 1/1/8:3     Collect-Stats
    Svc Id: 104  SAP : 1/1/8:4     Collect-Stats
    Svc Id: 105  SAP : 1/1/8:5     Collect-Stats
    Svc Id: 106  SAP : 1/1/8:6     Collect-Stats
    Svc Id: 107  SAP : 1/1/8:7     Collect-Stats
    Svc Id: 108  SAP : 1/1/8:8     Collect-Stats
    Svc Id: 109  SAP : 1/1/8:9     Collect-Stats
...
==============================================================================
A:ALA-1#
```

```
A:ALA-1# show log accounting-policy network
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
==============================================================================
A:ALA-1#
```

```
A:ALA-1# show log accounting-policy access
==============================================================================
Accounting Policies
==============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 complete-service-ingress-egress
==============================================================================
A:ALA-1#
```

accounting-records

Syntax **accounting-records**

Context show>log

Description This command displays accounting policy record names.

Output **Accounting Records Output.** The following table describes accounting records output fields.

Table 39: Accounting Policy Output Fields

Label	Description
Record #	The record ID that uniquely identifies the accounting policy, expressed as a decimal integer.
Record Name	The accounting record name.
Def. Interval	The default interval, in minutes, in which statistics are collected and written to their destination.

Sample Output

```
A:ALA-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
9        compact-service-ingress-octets    5
10       combined-service-ingress          5
11       combined-network-ing-egr-octets   15
12       combined-service-ing-egr-octets   5
13       complete-service-ingress-egress   5
14       combined-sdp-ingress-egress       5
15       complete-sdp-ingress-egress       5
16       complete-subscriber-ingress-egress 5
17       aa-protocol                       15
18       aa-application                    15
19       aa-app-group                      15
20       aa-subscriber-protocol            15
21       aa-subscriber-application         15
22       aa-subscriber-app-group           15
==========================================================
A:ALA-1#
```

applications

Syntax **applications**

Context show>log

Description This command displays a list of all application names that can be used in event-control and filter commands.

Output **Sample Output**

```
A:ALA-1# show log applications
==================================
Log Event Application Names
==================================
Application Name
----------------------------------
APS
ATM
BGP
CCAG
CFLOWD
CHASSIS
CPMHWFILTER
DHCP
DEBUG
DOT1X
FILTER
IGMP
IGMP_SNOOPING
IP
ISIS
```

```
LAG
LDP
LOGGER
MIRROR
MPLS
OAM
OSPF
PIM
PORT
PPP
QOS
RIP
ROUTE_POLICY
RSVP
SECURITY
SNMP
STP
SVCMGR
SYSTEM
USER
VRRP
VRTR
==================================
A:ALA-1#
```

event-control

Syntax **event-control** [**application** [*event-name* **|** *event-number*]]

Context show>log

Description This command displays event control settings for events including whether the event is suppressed or generated and the severity level for the event.

If no options are specified all events, alarms and traps are listed.

Parameters **application —** Only displays event control for the specified application.

Default All applications.

Values aps, atm, bgp, cflowd, chassis, debug, dhcp, efm_oam, filter, gsmp, igmp, igmp_snooping, ip, isis, lag, ldp, logger, mc_redundancy, mirror, mpls, ntp, oam, ospf, pim, port, ppp, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr

event-name — Only displays event control for the named application event.

Default All events for the application.

event-number — Only displays event control for the specified application event number.

Default All events for the application.

Output **Show Event Control Output —** The following table describes the output fields for the event control.

Label	Description
`Application`	The application name.
`ID#`	The event ID number within the application. `L ID#` — An “L” in front of an ID represents event types that do not generate an associated SNMP notification. Most events do generate a notification, only the exceptions are marked with a preceding “L”.
`Event Name`	The event name.
`P`	`CL` — The event has a cleared severity/priority. `CR` — The event has critical severity/priority. `IN` — The event has indeterminate severity/priority. `MA` — The event has major severity/priority. `MI` — The event has minor severity/priority. `WA` — The event has warning severity/priority.
`g/s`	`gen` — The event will be generated/logged by event control. `sup` — The event will be suppressed/dropped by event control. `thr` — Specifies that throttling is enabled.
`Logged`	The number of events logged/generated.
`Dropped`	The number of events dropped/suppressed.

Sample Output

```
A:gal171# show log event-control
=======================================================================
Log Events
=======================================================================
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
-----------------------------------------------------------------------
APS:
   2001 apsEventSwitchover               MI  thr         20         123
   2002 apsEventModeMismatch             MI  gen          0           0
   2003 apsEventChannelMismatch          MI  sup          0           0
   2004 apsEventPSBF                     MI  thr          0           0
   2005 apsEventFEPLF                    MI  thr          0           0
...
ATM:
   2004 tAtmTcSubLayerDown               MI  gen          0           0
   2005 tAtmTcSubLayerClear              MI  gen          0           0
L  2006 atmVclStatusChange               WA  gen          0           0
...
BGP:
   2001 bgpEstablished                   MI  gen          0           0
   2002 bgpBackwardTransition            WA  gen          0           0
   2003 tBgpMaxPrefix90                  WA  gen          0           0
   2004 tBgpMaxPrefix100                 CR  gen          0           0
L  2005 sendNotification                 WA  gen          0           0
L  2006 receiveNotification              WA  gen          0           0
L  2007 bgpInterfaceDown                 WA  gen          0           0
L  2008 bgpConnNoKA                      WA  gen          0           0
L  2009 bgpConnNoOpenRcvd                WA  gen          0           0
L  2010 bgpRejectConnBadLocAddr          WA  gen          0           0
L  2011 bgpRemoteEndClosedConn           WA  gen          0           0
L  2012 bgpPeerNotFound                  WA  gen          0           0
L  2013 bgpConnMgrTerminated             WA  gen          0           0
L  2014 bgpTerminated                    WA  gen          0           0
L  2015 bgpNoMemoryPeer                  CR  gen          0           0
L  2016 bgpVariableRangeViolation        WA  gen          0           0
L  2017 bgpCfgViol                       WA  gen          0           0
CFLOWD:
   2001 cflowdCreated                    MI  gen          0           0
   2002 cflowdCreateFailure              MA  gen          0           0
   2003 cflowdDeleted                    MI  gen          0           0
   2004 cflowdStateChanged               MI  gen          0           0
   2005 cflowdCleared                    MI  gen          0           0
   2006 cflowdFlowCreateFailure          MI  gen          0           0
   2007 cflowdFlowFlushFailure           MI  gen          0           0
   2008 cflowdFlowUnsuppProto            MI  sup          0           0
CCAG:
...
CHASSIS:
   2001 cardFailure                      MA  gen          0           0
   2002 cardInserted                     MI  gen          4           0
   2003 cardRemoved                      MI  gen          0           0
   2004 cardWrong                        MI  gen          0           0
   2005 EnvTemperatureTooHigh            MA  gen          0           0
...
CPMHWFILTER:
DHCP:
   2001 sdpTlsDHCPSuspiciousPcktRcvd     WA  gen          0           0
   2002 sapTlsDHCPLseStEntriesExceeded   WA  gen          0           0
   2003 sapTlsDHCPLeaseStateOverride     WA  gen          0           0
   2004 sapTlsDHCPSuspiciousPcktRcvd     WA  gen          0           0
   2005 svcTlsDHCPLseStRestoreProblem    WA  gen          0           0
   2006 svcTlsDHCPLseStatePopulateErr    WA  gen          0           0
   2007 tmnxVRtrDHCPLseStsExceeded       WA  gen          0           0
   2008 tmnxVRtrDHCPLeaseStateOverride   WA  gen          0           0
   2009 tmnxVRtrDHCPSuspiciousPcktRcvd   WA  gen          0           0
   2010 tmnxVRtrDHCPLseStRestoreProblem  WA  gen          0           0
   2011 tmnxVRtrDHCPLseStatePopulateErr  WA  gen          0           0
DEBUG:
L  2001 traceEvent                       MI  gen          0           0
DOT1X:
FILTER:
   2001 filterPBRPacketsDropped          MI  gen          0           0
IGMP:
   2001 vRtrIgmpIfRxQueryVerMismatch     WA  gen          0           0
   2002 vRtrIgmpIfCModeRxQueryMismatch   WA  gen          0           0
IGMP_SNOOPING:
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
ISIS:
   2001 vRtrIsisDatabaseOverload         WA  gen          0           0
   2002 vRtrIsisManualAddressDrops       WA  gen          0           0
   2003 vRtrIsisCorruptedLSPDetected     WA  gen          0           0
   2004 vRtrIsisMaxSeqExceedAttempt      WA  gen          0           0
   2005 vRtrIsisIDLenMismatch            WA  gen          0           0
   2006 vRtrIsisMaxAreaAddrsMismatch     WA  gen          0           0
....
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
VRRP:
   2001 vrrpTrapNewMaster                MI  gen          0           0
   2002 vrrpTrapAuthFailure              MI  gen          0           0
   2003 tmnxVrrpIPListMismatch           MI  gen          0           0
   2004 tmnxVrrpIPListMismatchClear      MI  gen          0           0
   2005 tmnxVrrpMultipleOwners           MI  gen          0           0
   2006 tmnxVrrpBecameBackup             MI  gen          0           0
L  2007 vrrpPacketDiscarded              MI  gen          0           0
VRTR:
   2001 tmnxVRtrMidRouteTCA              MI  gen          0           0
   2002 tmnxVRtrHighRouteTCA             MI  gen          0           0
   2003 tmnxVRtrHighRouteCleared         MI  gen          0           0
   2004 tmnxVRtrIllegalLabelTCA          MA  gen          0           0
   2005 tmnxVRtrMcastMidRouteTCA         MI  gen          0           0
   2006 tmnxVRtrMcastMaxRoutesTCA        MI  gen          0           0
   2007 tmnxVRtrMcastMaxRoutesCleared    MI  gen          0           0
   2008 tmnxVRtrMaxArpEntriesTCA         MA  gen          0           0
   2009 tmnxVRtrMaxArpEntriesCleared     MI  gen          0           0
   2011 tmnxVRtrMaxRoutes                MI  gen          0           0
=======================================================================
A:ALA-1#


A:ALA-1# show log event-control ospf
=======================================================================
Log Events
=======================================================================
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
-----------------------------------------------------------------------
   2001 ospfVirtIfStateChange            WA  gen          0           0
   2002 ospfNbrStateChange               WA  gen          1           0
   2003 ospfVirtNbrStateChange           WA  gen          0           0
   2004 ospfIfConfigError                WA  gen          0           0
   2005 ospfVirtIfConfigError            WA  gen          0           0
   2006 ospfIfAuthFailure                WA  gen          0           0
   2007 ospfVirtIfAuthFailure            WA  gen          0           0
   2008 ospfIfRxBadPacket                WA  gen          0           0
   2009 ospfVirtIfRxBadPacket            WA  gen          0           0
   2010 ospfTxRetransmit                 WA  sup          0           0
   2011 ospfVirtIfTxRetransmit           WA  sup          0           0
   2012 ospfOriginateLsa                 WA  sup          0         404
   2013 ospfMaxAgeLsa                    WA  gen          3           0
   2014 ospfLsdbOverflow                 WA  gen          0           0
   2015 ospfLsdbApproachingOverflow      WA  gen          0           0
   2016 ospfIfStateChange                WA  gen          2           0
   2017 ospfNssaTranslatorStatusChange   WA  gen          0           0
   2018 vRtrOspfSpfRunsStopped           WA  gen          0           0
   2019 vRtrOspfSpfRunsRestarted         WA  gen          0           0
   2020 vRtrOspfOverloadEntered          WA  gen          1           0
   2021 vRtrOspfOverloadExited           WA  gen          0           0
   2022 ospfRestartStatusChange          WA  gen          0           0
   2023 ospfNbrRestartHelperStatusChange WA  gen          0           0
   2024 ospfVirtNbrRestartHelperStsChg   WA  gen          0           0
=======================================================================
A:ALA-1#


A:ALA-1# show log event-control ospf ospfVirtIfStateChange
=======================================================================
Log Events
=======================================================================
Application
 ID#    Event Name                       P   g/s     Logged     Dropped
-----------------------------------------------------------------------
   2001 ospfVirtIfStateChange            WA  gen          0           0
=======================================================================
A:ALA-1#
```

file-id

Syntax **file-id** [*log-file-id*]

Context show>log

Description This command displays event file log information.

If no command line parameters are specified, a summary output of all event log files is displayed.

Specifying a file ID displays detailed information on the event file log.

Parameters *log-file-id* — Displays detailed information on the specified event file log.

Output **Log File Output —** The following table describes the output fields for a log file summary.

Label	Description
`file-id`	The log file ID.

Label	Description (Continued)
`rollover`	The rollover time for the log file which is how long in between partitioning of the file into a new file.
`retention`	The retention time for the file in the system which is how long the file should be retained in the file system.
`admin location`	The primary flash device specified for the file location. `none` — indicates no specific flash device was specified.
`backup location`	The secondary flash device specified for the file location if the admin location is not available. `none` — Indicates that no backup flash device was specified.
`oper location`	The actual flash device on which the log file exists.
`file-id`	The log file ID.
`rollover`	The rollover time for the log file which is how long in between partitioning of the file into a new file.
`retention`	The retention time for the file in the system which is how long the file should be retained in the file system.
`file name`	The complete pathname of the file associated with the log ID.
`expired`	Indicates whether or not the retention period for this file has passed.
`state`	`in progress` — Indicates the current open log file. `complete` — Indicates the old log file.

Sample Output

```
A:ALA-1# show log file-id
=============================================================
File Id List
=============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
-------------------------------------------------------------
1           60         4        cf1:      cf2:      cf1:
2           60         3        cf1:      cf3:      cf1:
3         1440        12        cf1:      none      cf1:
10        1440        12        cf1:      none      none
11        1440        12        cf1:      none      none
15        1440        12        cf1:      none      none
20        1440        12        cf1:      none      none
=============================================================
A:ALA-1#


A:ALA-1# show log file-id 10
=============================================================
File Id List
```

```
=============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
-------------------------------------------------------------
10   1440        12        cf3:      cf2:      cf1:
Description : Main
===============================================================
File Id 10 Location cf1:
===============================================================
file name                               expired   state
---------------------------------------------------------------
cf1:\log\log0302-20060501-012205        yes       complete
cf1:\log\log0302-20060501-014049        yes       complete
cf1:\log\log0302-20060501-015344        yes       complete
cf1:\log\log0302-20060501-015547        yes       in progress
=============================================================
A:ALA-1#
```

filter-id

Syntax **filter-id** [*filter-id*]

Context show>log

Description This command displays event log filter policy information.

Parameters *filter-id* — Displays detailed information on the specified event filter policy ID.

Output **Event Log Filter Summary Output —** The following table describes the output fields for event log filter summary information.

Table 40: Event Log Filter Summary Output Fields

Label	Description
`Filter Id`	The event log filter ID.
`Applied`	`no.` The event log filter is not currently in use by a log ID.
	`yes.` The event log filter is currently in use by a log ID.
`Default Action`	`drop.` The default action for the event log filter is to drop events not matching filter entries.
	`forward.` The default action for the event log filter is to forward events not matching filter entries.
`Description`	The description string for the filter ID.

Sample Output

```
*A:ALA-48>config>log# show log filter-id
```

```
=============================================================================
Log Filters
=============================================================================
Filter Applied Default Description
Id             Action
-----------------------------------------------------------------------------
1      no      forward
5      no      forward
10     no      forward
1001   yes     drop    Collect events for Serious Errors Log
=============================================================================
*A:ALA-48>config>log#
```

Event Log Filter Detailed Output — The following table describes the output fields for detailed event log filter information .

Table 41: Event Log Filter Detail Output Fields

Label	Description
`Filter-id`	The event log filter ID.
`Applied`	`no` — The event log filter is not currently in use by a log ID.
	`yes` — The event log filter is currently in use by a log ID.
`Default Action`	`drop` — The default action for the event log filter is to drop events not matching filter entries.
	`forward` — The default action for the event log filter is to forward events not matching filter entries.
`Description` (Filter-id)	The description string for the filter ID.

.

Table 42: Log Filter Match Criteria Output Fields

Label	Description
`Entry-id`	The event log filter entry ID.
`Action`	`default` — There is no explicit action for the event log filter entry and the filter’s default action is used on matching events.
	`drop` — The action for the event log filter entry is to drop matching events.
	`forward` — The action for the event log filter entry is to forward matching events.

`Description`
`(Entry-id)`
	The description string for the event log filter entry.

Table 42: Log Filter Match Criteria Output Fields (Continued)

Label	Description
`Application`	The event log filter entry application match criterion.
`Event Number`	The event log filter entry application event ID match criterion.
`Severity`	`cleared` — The log event filter entry application event severity cleared match criterion. `indeterminate` — The log event filter entry application event severity indeterminate match criterion. `critical` — The log event filter entry application event severity critical match criterion. `major` — The log event filter entry application event severity cleared match criterion. `minor` — The log event filter entry application event severity minor match criterion. `warning` — The log event filter entry application event severity warning match criterion.
`Subject`	Displays the event log filter entry application event ID subject string match criterion.
`Router`	Displays the event log filter entry application event ID **router** *router-instance* string match criterion.
`Operator`	There is an operator field for each match criteria: application, event number, severity, and subject. `equal` — Matches when equal to the match criterion. `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.

Sample Output

```
*A:ALA-48>config>log# show log filter-id 1001
===============================================================================
Log Filter
==========================================================================
Filter-id     : 1001     Applied       : yes      Default Action: drop
Description   : Collect events for Serious Errors Log
--------------------------------------------------------------------------
Log Filter Match Criteria
--------------------------------------------------------------------------
Entry-id      : 10                      Action        : forward
Application   :                         Operator      : off
Event Number  : 0                       Operator      : off
Severity      : major                   Operator      : greaterThanOrEqual
Subject       :                         Operator      : off
Match Type    : exact string                          :
Router        :                         Operator      : off
Match Type    : exact string                          :
Description   : Collect only events of major severity or higher
--------------------------------------------------------------------------
==========================================================================
*A:ALA-48>config>log#
```

log-collector

Syntax **log-collector**

Context show>log

Description Show log collector statistics for the main, security, change and debug log collectors.

Output **Log-Collector Output —** The following table describes log-collector output fields.

Table 43: Show Log-Collector Output Fields

Label	Description
`<Collector Name>`	`Main` — The main event stream contains the events that are not explicitly directed to any other event stream. `Security` — The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. `Change` — The change event stream contains all events that directly affect the configuration or operation of this node. `Debug` — The debug-trace stream contains all messages in the debug stream.
`Dest. Log ID`	Specifies the event log stream destination.
`Filter ID`	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.

Table 43: Show Log-Collector Output Fields (Continued)

Label	Description
`Status`	`Enabled` — Logging is enabled. `Disabled` — Logging is disabled.
`Dest. Type`	`Console` — A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether a user is logged in to the console or not. A user logged in to the console device or connected to the CLI via a remote telnet or SSH session can also create a log with a destination type of 'session'. Events are displayed to the session device until the user logs off. When the user logs off, the 'session' type log is deleted. `Syslog` — All selected log events are sent to the syslog address. `SNMP traps` — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables. `File` — All selected log events will be directed to a file on one of the CPM's compact flash disks. `Memory` — All selected log events will be directed to an in-memory storage area.

Sample Output

```
A:ALA-1# show log log-collector
===============================================================================
Log Collectors
===============================================================================
Main                Logged   : 1224                Dropped  : 0
  Dest Log Id: 99    Filter Id: 0      Status: enabled    Dest Type: memory
  Dest Log Id: 100   Filter Id: 1001   Status: enabled    Dest Type: memory

Security            Logged   : 3                   Dropped  : 0

Change              Logged   : 3896                Dropped  : 0

Debug               Logged   : 0                   Dropped  : 0

===============================================================================
A:ALA-1#
```

log-id

Syntax **log-id** [*log-id*] [**severity** *severity-level*] [**application** *application*] [**sequence** *from-seq* [*to-seq*]] [**count** *count*] [**router** *router-instance* [**expression**]] [**subject** *subject* [**regexp**]] [**ascending | descending**]

Context show>log

Description This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.

If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.

If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.

Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.

Parameters *log-id* — Displays the contents of the specified file log or memory log ID. The log ID must have a destination of an SNMP or file log or a memory log for this parameter to be used.

Default Displays the event log summary

Values 1 — 99

severity *severity-level* — Displays only events with the specified and higher severity.

Default All severity levels

Values cleared, indeterminate, critical, major, minor, warning

application *application* — Displays only events generated by the specified application.

Default All applications

Values aps, atm, bgp, cflowd, chassis, dhcp, debug, filter, igmp, ip, isis, lag, ldp, logger, mirror, mpls, oam, ospf, pim, port, ppp, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr, ospf_ng|ntp

expression — Specifies to use a regular expression as match criteria for the router instance string.

sequence *from-seq* [*to-seq*] — Displays the log entry numbers from a particular entry sequence number (*from-seq*) to another sequence number (*to-seq*). The *to-seq* value must be larger than the *from-seq* value.

If the *to-seq* number is not provided, the log contents to the end of the log is displayed unless the **count** parameter is present in which case the number of entries displayed is limited by the **count**.

Default All sequence numbers

Values 1 — 4294967295

count *count* — Limits the number of log entries displayed to the *number* specified.

Default All log entries

Values 1 — 4294967295

router-instance — Specifies a router name up to 32 characters to be used in the display criteria.

subject *subject* — Displays only log entries matching the specified text *subject* string. The subject is the object affected by the event, for example the port-id would be the subject for a link-up or link-down event.

regexp — Specifies to use a regular expression as parameters with the specified *subject* string..

ascending | **descending** — Specifies sort direction. Logs are normally shown from the newest entry to the oldest in **descending** sequence number order on the screen. When using the **ascending** parameter, the log will be shown from the oldest to the newest entry.

Default Descending

Output **Show Log-ID Output —** The following table describes the log ID field output.

Label	Description
`Log Id`	An event log destination.
`Source`	`no` — The event log filter is not currently in use by a log ID.
	`yes` — The event log filter is currently in use by a log ID.
`Filter ID`	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
`Admin State`	`Up` — Indicates that the administrative state is up.
	`Down` — Indicates that the administrative state is down.
`Oper State`	`Up` — Indicates that the operational state is up.
	`Down` — Indicates that the operational state is down.
`Logged`	The number of events that have been sent to the log source(s) that were forwarded to the log destination.
`Dropped`	The number of events that have been sent to the log source(s) that were not forwarded to the log destination because they were filtered out by the log filter.
`Dest. Type`	`Console` — All selected log events are directed to the system console. If the console is not connected, then all entries are dropped.
	`Syslog` — All selected log events are sent to the syslog address.
	`SNMP traps` — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables.
	`File` — All selected log events will be directed to a file on one of the CPM's compact flash disks.

Label	Description (Continued)
	Memory — All selected log events will be directed to an in-memory storage area.
Dest ID	The event log stream destination.
Size	The allocated memory size for the log.
Time format	The time format specifies the type of timestamp format for events sent to logs where log ID destination is either syslog or file. When the time format is UTC, timestamps are written using the Coordinated Universal Time value. When the time format is local, timestamps are written in the system's local time.

Sample Output

```
A:ALA-1# show log log-id
=====================================================================
Event Logs
=====================================================================
Log Source    Filter Admin Oper  Logged  Dropped Dest       Dest  Size
Id            Id     State State                 Type       Id
--------------------------------------------------------------------
1   none      none   up    down  52      0       file       10     N/A
2   C         none   up    up    41      0       syslog     1      N/A
99  M         none   up    up    2135    0       memory            500
=====================================================================
A:ALA-1#
```

Sample Memory or File Event Log Contents Output

```
A:gal171# show log log-id 99
===============================================================================
Event Log 99
===============================================================================
Description : Default System Log
Memory Log contents  [size=500   next event=70  (not wrapped)]

69 2007/01/25 18:20:40.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

68 2007/01/25 17:48:38.16 UTC WARNING: SYSTEM #2006 Base LOGGER
"New event throttle interval 10, configuration modified"

67 2007/01/25 00:34:53.97 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

66 2007/01/24 22:59:22.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

65 2007/01/24 02:08:47.92 UTC CRITICAL: SYSTEM #2029 Base Redundancy
```

```
"The active CPM card A is operating in singleton mode.  There is no standby CPM card."
...
===============================================================================
A:gal171


A:NS061550532>config>log>snmp-trap-group# show log log-id 1
===============================================================================
Event Log 1
===============================================================================
SNMP Log contents  [size=100   next event=3  (not wrapped)]
Cannot send to SNMP target address 10.1.1.1.
Waiting to replay starting from event #2

14 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2007 Base VR 1:
"Instance is in administrative state: inService, operational state: inService"

13 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2008 Base VR 1:
"Interface linkToIxia is in administrative state: inService, operational state:
inService"
....
===============================================================================
A:NS061550532>config>log>snmp-trap-group#
```

snmp-trap-group

Syntax **snmp-trap-group** [*log-id*]

Context show>log

Description This command displays SNMP trap group configuration information.

Parameters *log-id* — Displays only SNMP trap group information for the specified trap group log ID.

Values 1 — 99

Output **SNMP Trap Group Output —** The following table describes SNMP trap group output fields.

Table 44: SNMP Trap Group Output Fields

Label	Description
`Log-ID`	The log destination ID for an event stream.
`Address`	The IP address of the trap receiver,
`Port`	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
`Version`	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are snmpv1, snmpv2c, snmpv3.
`Community`	The community string required by **snmpv1** or **snmpv2c** trap receivers.

Table 44: SNMP Trap Group Output Fields (Continued)

Label	Description
`Security-Level`	The required authentication and privacy levels required to access the views on this node.
`Replay`	Indicates whether or not the replay parameter has been configured, enabled or disabled, for the trap-target address.
`Replay from`	Indicates the sequence ID of the first missed notification that will be replayed when a route is added to the routing table by which trap-target address can be reached. If no notifications are waiting to be replayed this field shows n/a.
`Last Replay`	Indicates the last time missed events were replayed to the trap-target address. If no events have ever been replayed this field shows never.

Sample SNMP Trap Group Output

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : ntt-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : ntttesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : ntttesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
A:SetupCLI>config>log>snmp-trap-group#
```

syslog

Syntax **syslog** [*syslog-id*]

Context show>log

Description This command displays syslog event log destination summary information or detailed information on a specific syslog destination.

Parameters *syslog-id* — Displays detailed information on the specified syslog event log destination.

Values 1 — 10

Output **Syslog Event Log Destination Summary Output —** The following table describes the syslog output fields.

Table 45: Show Log Syslog Output Fields

Label	Description
`Syslog ID`	The syslog ID number for the syslog destination.
`IP Address`	The IP address of the syslog target host.
`Port`	The configured UDP port number used when sending syslog messages.
`Facility`	The facility code for messages sent to the syslog target host.
`Severity Level`	The syslog message severity level threshold.
`Below Level Dropped`	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.
`Prefix Present`	`Yes` — A log prefix was prepended to the syslog message sent to the syslog host. `No` — A log prefix was not prepended to the syslog message sent to the syslog host.
`Description`	A text description stored in the configuration file for a configuration context.
`LogPrefix`	The prefix string prepended to the syslog message.
`Log-id`	Events are directed to this destination.

Sample Syslog Event Log Destination Summary Output

```
*A:ALA-48>config>log# show log syslog
===============================================================================
Syslog Target Hosts
===============================================================================
Id     Ip Address                                       Port        Sev Level
         Below Level Drop                                 Facility    Pfx Level
```

```
-------------------------------------------------------------------------------
2      unknown                                         514         info
         0                                               local7      yes
3      unknown                                         514         info
         0                                               local7      yes
5      unknown                                         514         info
         0                                               local7      yes
10     unknown                                         514         info
         0                                               local7      yes
===============================================================================
*A:ALA-48>config>log#


*A:MV-SR>config>log# show log syslog 1
===============================================================================
Syslog Target 1
===============================================================================
IP Address       : 192.168.15.22
Port             : 514
Log-ids          : none
Prefix           : Sr12
Facility         : local1
Severity Level   : info
Prefix Level     : yes
Below Level Drop : 0
Description      : Linux Station Springsteen
===============================================================================
*A:MV-SR>config>log#
```

Clear Commands

log

Syntax **log** *log-id*

Context clear

Description Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.

This command is only applicable to event logs that are directed to file destinations and memory destinations.

SNMP, syslog and console/session logs are not affected by this command.

Parameters *log-id.* The event log ID to be initialized/rolled over.

Values 1 — 100

Facility Alarms

In This Chapter

This chapter provides information about configuring event and accounting logs in the 7750 SR.

Topics in this chapter include:

Facility Alarms Overview

Facility Alarms provide a useful tool for operators to easily track and display the basic status of their equipment facilities.

CLI display (show routines) allows the 7750 SR operator to easily identify current facility alarm conditions and recently cleared alarms without searching event logs or monitoring various card and port show commands to determine the health of managed objects in the system such as cards and ports.

The SR-OS alarm model is based on RFC 3877, *Alarm Management Information Base (MIB)*, (which evolved from the IETF DISMAN drafts).

Facility Alarms vs. Log Events

Facility Alarms are different than (log) events. Events are a single point in time and are generally stateless. Facility Alarms have a state (at least two states: active and clear) and duration and can be modelled with state transition events (raised, cleared).

The Facility Alarms module processes log events in order to generate the raised and cleared state for the alarms. If a raising log event is suppressed under event-control, then the associated Alarm will not be raised. If a clearing log event is suppressed under event-control, then it is still processed for the purpose of clearing the associated alarm. Log event filtering, throttling and discarding of events during overload do not affect Facility Alarm processing. Log events are processed by the Facility Alarm module before they are discarded in all cases.

Figure 7 illustrates the relationship of log events, alarms and the LEDs.

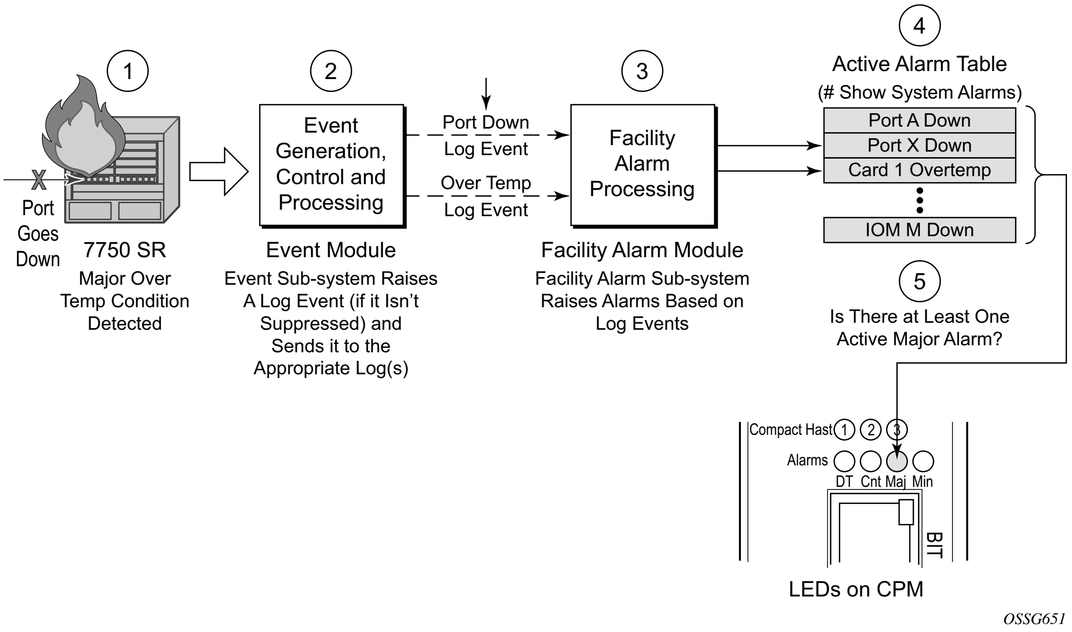
1
Port Goes Down
7750 SR
Major Over Temp Condition Detected
2
Event Generation, Control and Processing
Event Module
Event Sub-system Raises A Log Event (if it Isn't Suppressed) and Sends it to the Appropriate Log(s)
Port Down Log Event
Over Temp Log Event
3
Facility Alarm Processing
Facility Alarm Module
Facility Alarm Sub-system Raises Alarms Based on Log Events
4
Active Alarm Table
(# Show System Alarms)
Port A Down
Port X Down
Card 1 Overtemp
IOM M Down
5
Is There at Least One Active Major Alarm?
Compact Hast
1
2
3
Alarms
DT
Cnt
Maj
Min
BIT
LEDs on CPM
OSSG651

Figure 7: Log Events, Alarms and LEDs

Facility Alarms are different and independent functionality from other uses of the term “alarm” in SR-OS such as:

- Log events that use the term **alarm** (tmnxEqPortSonetAlarm)
- **configure card fp hi-bw-mcast-src** [**alarm**]
- **configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms**
- **configure port ethernet report-alarm**

- **configure system thresholds no memory-use-alarm**
- **configure system thresholds rmon no alarm**
- **configure system security cpu-protection policy alarm**

Facility Alarm Severities and Alarm LED Behavior

The Alarm LEDs on the CPM/CCM reflects the current status of the Facility Alarms:

- The Critical Alarm LED is lit if there is 1 or more active Critical Facility Alarms
- Similarly with the Major and Minor alarm LEDs
- The OT Alarm LED is not controlled by the Facility Alarm module

The supported alarm severities are as follows:

- Critical (with an associated LED on the CPM/CCM)
- Major (with an associated LED on the CPM/CCM)
- Minor (with an associated LED on the CPM/CCM)
- Warning (no LED)

Alarms inherit their severity from the raising event.

Log events that are a raising event for a facility alarm configured with a severity of "indeterminate" or "cleared" will result in those alarms not being raised (but clearing events are processed in order to clear alarms regardless of the severity of the clearing event).

Changing the severity of a raising event only affects subsequent occurrences of that event and alarms. Alarms that are already raised when their raising event severity is changed maintain their original severity.

Facility Alarm Hierarchy

Facility Alarms for “children” objects is not raised for failure of a “parent” object. For example, when an IOM fails (or is “shutdown”) there is not a set of port alarms raised.

When a parent alarm is cleared, children alarms that are still in occurrence on the node appears in the active alarms list. e.g. When a port fails there is a port alarm, but if the MDA is later shutdown the port alarm is cleared (and a card alarm will be active for the MDA). If the MDA comes back into service, and the port is still down, then a port alarm becomes active once again.

The supported Facility Alarm hierarchy is as follows (parent objects that are “down” cause alarms in all children to be masked):

- CHASSIS -> CPM -> flash
- CHASSIS -> CCM -> flash
- CHASSIS -> fabric
- CHASSIS -> fan
- CHASSIS -> power supply
- CHASSIS -> IOM -> MDA -> port -> channel
- CHASSIS -> MCM -> MDA -> port -> channel

Note that a “masked” alarm is not the same as a “cleared” alarm. The cleared alarm queue does not display entries for previously raised alarms that are currently masked. If the masking event goes away, then the previously raised alarms will once again be visible in the active alarm queue.

Facility Alarm List

The following table(s) show the supported Facility Alarms.

Table 46: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event
7-2001-1	tmnxEqCardFailure	Class MDA Module: failed, reason: Mda 1 failed startup tests	tmnxChassisNotification Clear
7-2003-1	tmnxEqCardRemoved	Class CPM Module: removed	tmnxEqCardInserted
7-2004-1	tmnxEqWrongCard	Class IOM Module: wrong type inserted	tmnxChassisNotification Clear
7-2005-1	tmnxEnvTempTooHigh	Chassis 1: temperature too high	tmnxChassisNotification Clear
7-2006-1	tmnxEqFanFailure	Fan 2 failed	tmnxChassisNotification Clear
7-2007-1	tmnxEqPowerSupplyFailureOvt	Power supply 2 over temperature	tmnxChassisNotification Clear
7-2008-1	tmnxEqPowerSupplyFailureAc	Power supply 1 AC failure	tmnxChassisNotification Clear
7-2009-1	tmnxEqPowerSupplyFailureDc	Power supply 2 DC failure	tmnxChassisNotification Clear
7-2011-1	tmnxEqPowerSupplyRemoved	Power supply 1, power lost	tmnxEqPowerSupplyInserted
7-2017-1	tmnxEqSyncIfTimingHoldover	Synchronous Timing interface in holdover state	tmnxEqSyncIfTimingHoldoverClear
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Synchronous Timing interface, alarm los on reference 1	tmnxEqSyncIfTimingRef1AlarmClear
7-2019-2	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oof(2)'	Synchronous Timing interface, alarm oof on reference 1	same as 7-2019-1
7-2019-3	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	Synchronous Timing interface, alarm oopir on reference 1	same as 7-2019-1
7-2021-x	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2
7-2030-x	same as 7-2019-x but for the BITS input	same as 7-2019-x but for the BITS input	same as 7-2019-x but for the BITS input
7-2033-1	tmnxChassisUpgradeInProgress	Class CPM Module: software upgrade in progress	tmnxChassisUpgradeComplete

Table 46: Alarm, Alarm Name/Raising Event, Sample Details String and Clearing Event (Continued)

Alarm *1	Alarm Name/Raising Event	Sample Details String	Clearing Event
7-2050-1	tmnxEqPowerSupplyFailureInput	Power supply 1 input failure	tmnxChassisNotification Clear
7-2051-1	tmnxEqPowerSupplyFailureOutput	Power supply 1 output failure	tmnxChassisNotification Clear
7-2073-x	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input
3-2004-1	linkDown	Interface intf-towards-node-B22 is not operational	linkUp

Table 47: Alarm Name/Raising Event, Cause, Effect and Recovery

Alarm *1	Alarm Name/Raising Event	Cause	Effect	Recovery
7-2001-1	tmnxEqCardFailure	Generated when one of the cards in a chassis has failed. The card type may be IOM, Fabric, MDA, MCM, CCM, CPM module, compact flash module, etc. The reason is indicated in the details of the log event or alarm, and is also available in the tmnxChassisNotifyCardFailureReason attribute included in the SNMP notification.	The effect is dependant on the card that has failed. IOM or MDA failure will cause a loss of service for all services running on that IOM or MDA. A fabric failure can impact traffic to/from all cards.	Before taking any recovery steps collect a tech-support file, then try resetting (clear) the card. If that doesn't work then try removing and then re-inserting the card. If that doesn't work then replace the card.
7-2003-1	tmnxEqCardRemoved	Generated when a card is removed from the chassis. The card type may be IOM, Fabric, MDA, MCM, CCM, CPM module, compact flash module, etc.	The effect is dependant on the card that has been removed. IOM or MDA removal will cause a loss of service for all services running on that IOM or MDA. A fabric removal can impact traffic to/from all cards.	Before taking any recovery steps collect a tech-support file, then try re-inserting the card. If that doesn't work then replace the card.
7-2004-1	tmnxEqWrongCard	Generated when the wrong type of card is inserted into a slot of the chassis. Even though a card may be physically supported by the slot, it may have been administratively configured to allow only certain card types in a particular slot location. The card type may be IOM, Fabric, MDA, MCM, CPM module, etc.	The effect is dependant on the card that has been incorrectly inserted. Incorrect IOM or MDA insertion will cause a loss of service for all services running on that IOM or MDA.	Insert the correct card into the correct slot, and ensure the slot is configured for the correct type of card.

Table 47: Alarm Name/Raising Event, Cause, Effect and Recovery (Continued)

Alarm *1	Alarm Name/Raising Event	Cause	Effect	Recovery
7-2005-1	tmnxEnvTempTooHigh	Generated when the temperature sensor reading on an equipment object is greater than its configured threshold.	This could be causing intermittent errors and could also cause permanent damage to components.	Remove or power down the affected cards, or improve the cooling to the node. More powerful fan trays may also be required.
7-2006-1	tmnxEqFanFailure	Generated when one of the fans in a fan tray has failed.	This could be cause temperature to rise and resulting intermittent errors and could also cause permanent damage to components.	Replace the fan tray immediately, improve the cooling to the node, or reduce the heat being generated in the node by removing cards or powering down the node.
7-2007-1	tmnxEqPowerSupplyFailureOvt	Generated when the temperature sensor reading on a power supply module is greater than its configured threshold.	This could be causing intermittent errors and could also cause permanent damage to components.	Remove or power down the affected power supply module or improve the cooling to the node. More powerful fan trays may also be required. The power supply itself may be faulty so replacement may be necessary.
7-2008-1	tmnxEqPowerSupplyFailureAc	Generated when an AC failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.
7-2009-1	tmnxEqPowerSupplyFailureDc	Generated when an DC failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.
7-2011-1	tmnxEqPowerSupplyRemoved	Generated when one of the chassis's power supplies is removed.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	Re-insert the power supply.

Table 47: Alarm Name/Raising Event, Cause, Effect and Recovery (Continued)

Alarm *1	Alarm Name/Raising Event	Cause	Effect	Recovery
7-2017-1	tmnxEqSyncIfTimingHoldover	Generated when the synchronous equipment timing subsystem transitions into a holdover state.	Any node-timed ports will have very slow frequency drift limited by the central clock oscillator stability. The oscillator meets the holdover requirements of a Stratum 3 and G.813 Option 1 clock.	Address issues with the central clock input references.
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Generated when an alarm condition on the first timing reference is detected. The type of alarm (los, oof, etc) is indicated in the details of the log event or alarm, and is also available in the tmnxSyncIfTimingNotifyAlarm attribute included in the SNMP notification. The SNMP notification will have the same indices as those of the tmnxCpmCardTable.	Timing reference 1 cannot be used as a source of timing into the central clock.	Address issues with the signal associated with timing reference 1.
7-2019-2	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oof(2)'	same as 7-2019-1	same as 7-2019-1	same as 7-2019-1
7-2019-3	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	same as 7-2019-1	same as 7-2019-1	same as 7-2019-1
7-2021-x	same as 7-2019-x but for ref2	same as 7-2019-x but for the second timing reference	same as 7-2019-x but for the second timing reference	same as 7-2019-x but for the second timing reference
7-2030-x	same as 7-2019-x but for the BITS input	same as 7-2019-x but for the BITS timing reference	same as 7-2019-x but for the BITS timing reference	same as 7-2019-x but for the BITS timing reference

Table 47: Alarm Name/Raising Event, Cause, Effect and Recovery (Continued)

Alarm *1	Alarm Name/Raising Event	Cause	Effect	Recovery
7-2033-1	tmnxChassisUpgradeInProgress	The tmnxChassisUpgradeInProgress notification is generated only after a CPM switchover occurs and the new active CPM is running new software, while the IOMs are still running old software. This is the start of the upgrade process. The tmnxChassisUpgradeInProgress notification will continue to be generated every 30 minutes while at least one IOM is still running older software.	A s/w mismatch between the CPM and IOM is generally fine for a short duration (during an upgrade) but may not allow for correct long term operation.	Complete the upgrade of all IOMs.
7-2050-1	tmnxEqPowerSupplyFailureInput	Generated when an input failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.
7-2051-1	tmnxEqPowerSupplyFailure Output	Generated when an output failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.
7-2073-x	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS 2 timing reference	same as 7-2019-x but for the BITS 2 timing reference	same as 7-2019-x but for the BITS 2 timing reference
3-2004-1	linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state).	The indicated interface is taken down.	If the ifAdminStatus is down then the interface state is deliberate and there is no recovery. If the ifAdminStatus is up then try to determine that cause of the interface going down: cable cut, distal end went down, etc.

The linkDown Facility Alarm is supported for the following objects:

Table 48: linkDown Facility Alarm Support

Object	Supported?
Ethernet Ports	Yes
Sonet Section, Line and Path (POS)	Yes
TDM Ports (E1, T1, DS3) including CES MDAs/CMAs	Yes
TDM Channels (DS3 channel configured in an STM-1 port)	Yes
ATM Ports	Yes
Ethernet LAGs	No
APS groups	No
Bundles (MLPPP, IMA, etc)	No
ATM channels, Ethernet VLANs, Frame Relay DLCIs	No

Configuring Logging with CLI

This section provides information to configure logging using the command line interface.

Topics in this section include:

- Basic Facility Alarm Configuration on page 476
- Common Configuration Tasks on page 477

Basic Facility Alarm Configuration

The most facility alarm configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays an alarm configuration example.

```
A:ALA-12>config>system# alarms
#------------------------------------------
        no shutdown
        exit
----------------------------------------------
```

Common Configuration Tasks

The following sections are basic alarm tasks that can be performed.

- Configuring the Maximum Number of Alarms To Clear on page 477

Configuring the Maximum Number of Alarms To Clear

The number of alarms to clear can be configured using the command listed below.

Use the following CLI syntax to configure a log file:

CLI Syntax:
```
config>system
 alarms
    max-cleared max-alarms
```

The following displays facility alarm configuration example:

```
ALA-12>config>system# alarms
----------------------------------------------
...
    max-cleared 100
    exit
...
----------------------------------------------
```

Facility Alarms Command Reference

Command Hierarchies

- Facility Alarm Configuration Commands on page 479
- Show Commands on page 479

Facility Alarm Configuration Commands

```
config
    — system
        — alarms
            — max-cleared max-alarms
            — [no] shutdown
```

Show Commands

```
show
    — system
        — alarms  [cleared] [severity <severity-level>] [count <count>] [newer-than <days>]
```

Configuration Commands

Generic Commands

alarms

Syntax **alarms**

Context config>system

Description This command enters the context to configure facility alarm parameters.

max-cleared

Syntax **max-cleared <***max-alarms***>**

Context config>system>alarms

Description This command configures the maximum number of cleared alarms that the system will store and display.

Default 500

Parameters *max-alarms* — Specify the maximum number of cleared alarms.

shutdown

Syntax **[no] shutdown**

Context config>system>alarms

Description This command enables or disables the Facility Alarm functionality. When enabled, the Facility Alarm sub-system tracks active and cleared facility alarms and controls the Alarm LEDs on the CPMs/CFMs. When Facility Alarm functionality is enabled, the alarms are viewed using the `show system alarms` command(s).

Default no shutdown

Show Commands

alarms

Syntax **show system alarms [cleared] [severity <***severity-level***>] [count <***count***>] [newer-than <***days***>]**

Context show>system

Description This command displays facility alarms on the system.

Output **Facility Alarm Output —** The following table describes the alarms output fields.

Sample Output

Table 49: Show Facility Alarms Output Fields

Label	Description
`Index`	Alarm index number.
`Date/Time`	Date and time string for the alarm.
`Severity`	Severity level of the alarm.
`Alarm`	Alarm identifier.
`Resource`	Facility associated with the alarm.
`Details`	Description of the alarm.

```
A:Dut-A# show system alarms

===============================================================================
Alarms [Critical:1 Major:2 Minor:0 Warning:0 Total:3]
===============================================================================
Index      Date/Time               Severity     Alarm         Resource
   Details
-------------------------------------------------------------------------------
8          2011/04/01 18:36:43.80  MAJOR        7-2011-1      Power Supply 1
   Power supply 1, power lost

7          2011/04/01 18:35:57.00  MAJOR        7-2005-1      Chassis 1
   Chassis 1: temperature too high

6          2011/04/01 18:35:24.80  CRITICAL     7-2006-1      Fan 1
   Fan 1 failed
===============================================================================


Cleared alarms table:
```

```
A:Dut-A# show system alarms cleared

===============================================================================
Cleared Alarms [Size:500 Total:5 (not wrapped)]
===============================================================================
Index      Date/Time               Severity     Alarm         Resource
   Details
-------------------------------------------------------------------------------
5          2011/04/01 18:11:55.00  MAJOR        7-2005-1      Chassis 1
   Clear Chassis temperature too high alarm

3          2011/04/01 18:11:54.50  CRITICAL     7-2051-1      Power Supply 1
   Clear Power Supply failure

2          2011/04/01 18:11:54.40  CRITICAL     7-2050-1      Power Supply 1
   Clear Power Supply failure

4          2011/04/01 18:11:54.10  MINOR        7-2004-1      Fan 1
   Clear Fan wrong type failure

1          2011/04/01 18:11:54.00  CRITICAL     7-2007-1      Power Supply 1
   Clear Power Supply failure
===============================================================================
```

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery

IEEE 802.1d Bridging

IEEE 802.1p/Q VLAN Tagging

IEEE 802.1s Multiple Spanning Tree

IEEE 802.1w Rapid Spanning Tree Protocol

IEEE 802.1x Port Based Network Access Control

IEEE 802.1ad Provider Bridges

IEEE 802.1ah Provider Backbone Bridges

IEEE 802.1ag Service Layer OAM

IEEE 802.3ah Ethernet in the First Mile

IEEE 802.1ak Multiple MAC Registration Protocol

IEEE 802.3 10BaseT

IEEE 802.3ad Link Aggregation

IEEE 802.3ae 10Gbps Ethernet

IEEE 802.3ah Ethernet OAM

IEEE 802.3u 100BaseTX

IEEE 802.3x Flow Control

IEEE 802.3z 1000BaseSX/LX

ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks

ITU-T G.8031 Ethernet linear protection switching

ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

OSPF

RFC 1765 OSPF Database Overflow

RFC 2328 OSPF Version 2

RFC 2370 Opaque LSA Support

RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospf-ospfv3-update-14.txt

RFC 3101 OSPF NSSA Option

RFC 3137 OSPF Stub Router Advertisement

RFC 3623 Graceful OSPF Restart – GR helper

RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2

RFC 4203 - Shared Risk Link Group (SRLG) sub-TLV

RFC 5185 OSPF Multi-Area Adjacency

RFC 3623 Graceful OSPF Restart — GR helper

RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2

RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

BGP

RFC 1397 BGP Default Route Advertisement

RFC 1772 Application of BGP in the Internet

RFC 1965 Confederations for BGP

RFC 1997 BGP Communities Attribute

RFC 2385 Protection of BGP Sessions via MD5

RFC 2439 BGP Route Flap Dampening

RFC 2547bis BGP/MPLS VPNs

RFC 2918 Route Refresh Capability for BGP-4

RFC 3107 Carrying Label Information in BGP-4

RFC 3392 Capabilities Advertisement with BGP4

RFC 4271 BGP-4 (previously RFC 1771)

RFC 4360 BGP Extended Communities Attribute

RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)

RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)

RFC 4486 Subcodes for BGP Cease Notification Message

RFC 4577 OSPF as the Provider/ Customer Edge Protocol for BGP/ MPLS IP Virtual Private Networks (VPNs)

RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

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

RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)

RFC 4893 BGP Support for Four-octet AS Number Space

RFC 5004 Avoid BGP Best Path Transitions from One External to Another

RFC 5065 Confederations for BGP (obsoletes 3065)

RFC 5291 Outbound Route Filtering Capability for BGP-4

RFC 5575 Dissemination of Flow Specification Rules

RFC 5668 4-Octet AS Specific BGP Extended Community

draft-ietf-idr-add-paths

draft-ietf-idr-best-external

IS-IS

RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)

RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments

RFC 2763 Dynamic Hostname Exchange for IS-IS

RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS

RFC 2973 IS-IS Mesh Groups

RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

RFC 3567 Intermediate System to Intermediate System (ISIS) Cryptographic Authentication

RFC 3719 Recommendations for Interoperable Networks using IS-IS

RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)

RFC 3787 Recommendations for Interoperable IP Networks

RFC 3847 Restart Signaling for IS-IS – GR helper

RFC 4205 for Shared Risk Link Group (SRLG) TLV

draft-ietf-isis-igp-p2p-over-lan-05.txt

IPSec

RFC 2401 Security Architecture for the Internet Protocol

RFC 2409 The Internet Key Exchange (IKE)

RFC 3706 IKE Dead Peer Detection

RFC 3947 Negotiation of NAT-Traversal in the IKE

RFC 3948 UDP Encapsulation of IPsec ESP Packets

draft-ietf-ipsec-isakmp-xauth-06.txt – Extended Authentication within ISAKMP/Oakley (XAUTH)

draft-ietf-ipsec-isakmp-modecfg-05.txt – The ISAKMP Configuration Method

IPv6

RFC 1981 Path MTU Discovery for IPv6

RFC 2375 IPv6 Multicast Address Assignments

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

RFC 2461 Neighbor Discovery for IPv6

RFC 2462 IPv6 Stateless Address Auto configuration

RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing

RFC 2710 Multicast Listener Discovery (MLD) for IPv6RFC 2740 OSPF for IPv6

RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses

RFC 3315 Dynamic Host Configuration Protocol for IPv6

RFC 3587 IPv6 Global Unicast Address Format

RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol

RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6

RFC 4007 IPv6 Scoped Address Architecture

RFC 4193 Unique Local IPv6 Unicast Addresses

RFC 4291 IPv6 Addressing Architecture

RFC 4552 Authentication/Confidentiality for OSPFv3

RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

RFC 5072 IP Version 6 over PPP

RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

draft-ietf-isis-ipv6-05

draft-ietf-isis-wg-multi-topology-xx.txt

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)

RFC 2236 Internet Group Management Protocol, (Snooping)

RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

RFC 2362 Protocol Independent Multicast-Sparse Mode (PIMSM)

RFC 3618 Multicast Source Discovery Protocol (MSDP)

RFC 3446 Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)

RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast

RFC 4607 Source-Specific Multicast for IP

RFC 4608 Source-Specific Protocol Independent Multicast in 232/8

RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)

RFC 5186, Internet Group Management Protocol Version 3 (IGMPv3)/ Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction

draft-ietf-pim-sm-bsr-06.txt

draft-rosen-vpn-mcast-15.txt Multicast in MPLS/BGP IP VPNs

draft-ietf-mboned-msdp-mib-01.txt

draft-ietf-l3vpn-2547bis-mcast-07: Multicast in MPLS/BGP IP VPNs

draft-ietf-l3vpn-2547bis-mcast-bgp-05: BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

MPLS — General

RFC 2430 A Provider Architecture DiffServ & TE

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)

RFC 2597 Assured Forwarding PHB Group (rev3260)

RFC 2598 An Expedited Forwarding PHB

RFC 3031 MPLS Architecture

RFC 3032 MPLS Label Stack Encoding

RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks

RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

RFC 3140 Per-Hop Behavior Identification Codes

RFC 4905, Encapsulation methods for transport of layer 2 frames over MPLS

RFC 5332 MPLS Multicast Encapsulations

MPLS — LDP

RFC 3037 LDP Applicability

RFC 3478 Graceful Restart Mechanism for LDP – GR helper

RFC 5036 LDP Specification

RFC 5283 LDP extension for Inter-Area LSP

RFC 5443 LDP IGP Synchronization

draft-ietf-mpls-ldp-p2mp-05 LDP Extensions for Point-to-Multipoint and Multipoint-to-Multipoint LSP

draft-ietf-mpls-mldp-in-band-signaling-05 Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

MPLS/RSVP-TE

RFC 2702 Requirements for Traffic Engineering over MPLS

RFC2747 RSVP Cryptographic Authentication

RFC3097 RSVP Cryptographic Authentication

RFC 3209 Extensions to RSVP for Tunnels

RFC 3564 Requirements for Diff-Serv-aware TE

RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels

RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels

RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering

RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering

RFC 4127 Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering

RFC 4561 Definition of a RRO Node-Id Sub-Object

RFC 4875 Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)

RFC 5151 Inter-domain MPLS and GMPLS Traffic Engineering – RSVP-TE Extensions

RFC 5712 MPLS Traffic Engineering Soft Preemption

draft-newton-mpls-te-dynamic-overbooking-00 A Diffserv-TE Implementation Model to dynamically change booking factors during failure events

RFC 5817 Graceful Shutdown in GMPLS Traffic Engineering Networks

MPLS — OAM

RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

draft-ietf-mpls-p2mp-lsp-ping-06 Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping

RIP

RFC 1058 RIP Version 1

RFC 2082 RIP-2 MD5 Authentication

RFC 2453 RIP Version 2

TCP/IP

RFC 768 UDP

RFC 1350 The TFTP Protocol (Rev.

RFC 791 IP

RFC 792 ICMP

RFC 793 TCP

RFC 826 ARP

RFC 854 Telnet

RFC 951 BootP (rev)

RFC 1519 CIDR

RFC 1542 Clarifications and Extensions for the Bootstrap Protocol

RFC 1812 Requirements for IPv4 Routers

RFC 2347 TFTP option Extension

RFC 2328 TFTP Blocksize Option

RFC 2349 TFTP Timeout Interval and Transfer

Size option

RFC 2401 Security Architecture for Internet Protocol

RFC 2428 FTP Extensions for IPv6 and NATs

RFC 3596 DNS Extensions to Support IP version 6

draft-ietf-bfd-mib-00.txtBidirectional Forwarding Detection Management Information Base

RFC 5880 Bidirectional Forwarding Detection

RFC 5881 BFD IPv4 and IPv6 (Single Hop)

RFC 5883 BFD for Multihop Paths

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

PPP

RFC 1332 PPP IPCP

RFC 1377 PPP OSINLCP

RFC 1638/2878PPP BCP

RFC 1661 PPP (rev RFC2151)

RFC 1662 PPP in HDLC-like Framing

RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses

RFC 1989 PPP Link Quality Monitoring

RFC 1990 The PPP Multilink Protocol (MP)

RFC 1994 PPP Challenge Handshake

Authentication Protocol (CHAP)

RFC 2615 PPP over SONET/SDH

RFC 2516 A Method for Transmitting PPP Over Ethernet

RFC 2686 The Multi-Class Extension to Multi-Link PPP

Frame Relay

FRF.1.2 - PVC User-to-Network Interface (UNI) Implementation Agreement

FRF.5 - Frame Relay/ATM PVC Network Interworking Implementation

ANSI T1.617 Annex D, DSS1 — Signalling Specification For Frame Relay Bearer Service.

FRF2.2 -PVC Network-to- Network Interface (NNI) Implementation Agreement.

FRF.12 Frame Relay Fragmentation Implementation Agreement

FRF.16.1 Multilink Frame Relay UNI/ NNI Implementation Agreement

ITU-T Q.933 Annex A- Additional procedures for Permanent Virtual Connection (PVC) status management

ATM

RFC 1626 Default IP MTU for use over ATM AAL5

RFC 2514 Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management

RFC 2515 Definition of Managed Objects for ATM Management RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5

AF-TM-0121.000 Traffic Management Specification Version 4.1

ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95

ITU-T Recommendation I.432.1 – BISDN user-network interface – Physical layer specification: General characteristics

GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3

GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1

AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0

AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR

AF-PHY-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP

RFC 2131 Dynamic Host Configuration Protocol (REV)

RFC 3046 DHCP Relay Agent Information Option (Option 82)

RFC 1534 Interoperation between DHCP and BOOTP

VPLS

RFC 4762 Virtual Private LAN Services Using LDP

RFC5501: Requirements for Multicast Support in Virtual Private LAN Services (previously draft-ietf-l2vpn-vpls-mcast-reqts-04)

draft-ietf-l2vpn-vpls-mcast-reqts-04

draft-ietf-l2vpn-signaling-08

PSEUDOWIRE

RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)

RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)

RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atm-encap-10.txt)

RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)

RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietf-pwe3-frame-relay-07.txt)

RFC 4446 IANA Allocations for PWE3

RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)

RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge

draft-ietf-l2vpn-vpws-iw-oam-02.txt, OAM Procedures for VPWS Interworking

RFC6310, Pseudowire (PW) OAM Message Mapping

draft-ietf-l2vpn-arp-mediation-19.txt, ARP Mediation for IP Interworking of Layer 2 VPN

RFC6073, Segmented Pseudowire (draft-ietf-pwe3-segmented-pw-18.txt)

draft-ietf-pwe3-dynamic-ms-pw-14.txt, Dynamic Placement of Multi Segment Pseudo Wires

draft-ietf-pwe3-redundancy-bit-06.txt, Pseudowire Preferential Forwarding Status bit definition

draft-ietf-pwe3-redundancy-06.txt, Pseudowire (PW) Redundancy

RFC6391 Flow Aware Transport of Pseudowires over an MPLS PSN

MFA Forum 9.0.0 The Use of Virtual trunks for ATM/MPLS Control Plane Interworking

MFA Forum 12.0.0 Multiservice Interworking - Ethernet over MPLS

MFA forum 13.0.0 - Fault Management for Multiservice Interworking v1.0

MFA Forum 16.0.0 – Multiservice Interworking - IP over MPLS

ANCP/L2CP

RFC5851 ANCP framework

draft-ietf-ancp-protocol-02.txt ANCP Protocol

Voice /Video Performance

ITU-T G.107 The E Model- A computational model for use in planning.

ETSI TS 101 329-5 Annex E extensions-QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring

ITU-T Rec. P.564 - Conformance testing for voice over IP transmission quality assessment models

ITU-T G.1020 - Appendix I - Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks- Mean Absolute Packet Delay Variation.& Markov Models.

RFC 3550 Appendix A.8- RTP: A Transport Protocol for Real-Time Applications- Estimating the Interarrival Jitter

CIRCUIT EMULATION

RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

MEF-8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks, October 2004

RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks

SONET/SDH

ITU-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

RADIUS

RFC 2865 Remote Authentication Dial In User Service

RFC 2866 RADIUS Accounting

SSH

RFC 4250 The Secure Shell (SSH) Protocol

draft-ietf-secsh-architecture.txtSSH Protocol Architecture

draft-ietf-secsh-userauth.txt SSH Authentication Protocol

draft-ietf-secsh-transport.txt SSH Transport Layer Protocol

draft-ietf-secsh-connection.txt SSH Connection Protocol

draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

Timing

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008

ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.

GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005

ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.

ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.

ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information

ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function

M.3100/3120 Equipment and Connection Models

TMF 509/613 Network Connectivity Model

RFC 1157 SNMPv1

RFC 1215 A Convention for Defining Traps for use with the SNMP

RFC 1657 BGP4-MIB

RFC 1724 RIPv2-MIB

RFC 1850 OSPF-MIB

RFC 1907 SNMPv2-MIB

RFC 2011 IP-MIB

RFC 2012 TCP-MIB

RFC 2013 UDP-MIB

RFC 2138 RADIUS

RFC 2206 RSVP-MIB

RFC 2452 IPv6 Management Information Base for the Transmission Control Protocol

RFC 2454 IPv6 Management Information Base for the User Datagram Protocol

RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group

RFC 2558 SONET-MIB

RFC 2571 SNMP-Framework MIB

RFC 2572 SNMP-MPD-MIB

RFC 2573 SNMP-Target-&-notification-MIB

RFC 2574 SNMP-User-based-SMMIB

RFC 2575 SNMP-View-based ACM-MIB

RFC 2576 SNMP-Community-MIB

RFC 2665 EtherLike-MIB

RFC 2819 RMON-MIB

RFC 2863 IF-MIB

RFC 2864 Inverted-stack-MIB

RFC 2987 VRRP-MIB

RFC 3014 Notification-log MIB

RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol

RFC 3164 Syslog

RFC 3273 HCRMON-MIB

RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413 Simple Network Management Protocol (SNMP) Applications

RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3418 SNMP MIB

RFC 4292 IP-Forward-MIB

RFC 4293 MIB for the Internet Protocol

RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information

draft-ietf-ospf-mib-update-04.txt

draft-ietf-mpls-lsr-mib-06.txt

draft-ietf-mpls-te-mib-04.txt

draft-ietf-mpls-ldp-mib-07.txt

draft-ietf-isis-wg-mib-05.txt

IANA-IFType-MIB

IEEE8023-LAG-MIB

Proprietary MIBs

TIMETRA-APS-MIB.mib

TIMETRA-ATM-MIB.mib

TIMETRA-BGP-MIB.mib

TIMETRA-BSX-NG-MIB.mib

TIMETRA-CAPABILITY-7750-V4v0.mib

TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IGMP-MIB.mib
TIMETRA-ISIS-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-NG-BGP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-OSPF-NG-MIB.mib
TIMETRA-OSPF-V3-MIB.mib
TIMETRA-PIM-NG-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-RIP-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SUBSCRIBER-MGMTMIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRRP-MIB.mib
TIMETRA-VRTR-MIB.mib

Index