



Alcatel-Lucent 7450

ETHERNET SERVICE SWITCH | RELEASE 13.0.R1
SYSTEM MANAGEMENT GUIDE

Alcatel-Lucent – Proprietary & Confidential
Contains proprietary/trade secret information which is the property of Alcatel-Lucent. Not to be made available to, or copied or used by anyone who is not an employee of Alcatel-Lucent except when there is a valid non-disclosure agreement in place which covers such information and contains appropriate non-disclosure and limited use obligations.
Copyright 2015 © Alcatel-Lucent. All rights reserved.

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

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

Copyright 2015 Alcatel-Lucent.

All rights reserved.

Disclaimers

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

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

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

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

Table of Contents

Preface	13
About This Guide	13
Audience	13
List of Technical Publications	14
Technical Support	16
Getting Started	
In This Chapter	17
Alcatel-Lucent 7450 ESS Router Configuration Process	17
Security	
In This Chapter	19
Authentication, Authorization, and Accounting	20
Authentication	21
Local Authentication	22
RADIUS Authentication	22
TACACS+ Authentication	27
Authorization	28
Local Authorization	28
RADIUS Authorization	28
TACACS+ Authorization	29
Accounting	32
RADIUS Accounting	32
TACACS+ Accounting	32
Security Controls	34
When a Server Does Not Respond	34
Access Request Flow	35
CPU Protection	36
CPU Protection Extensions ETH-CFM	40
ETH-CFM Ingress Squelching	42
Distributed CPU Protection (DCP)	45
Applicability of Distributed CPU Protection	47
Log Events, Statistics, Status and SNMP support	48
DCP Policer Resource Management	49
Operational Guidelines and Tips	50
Vendor-Specific Attributes (VSAs)	51
Other Security Features	52
Secure Shell (SSH)	52
SSH PKI Authentication	53
Key Generation	53
Per Peer CPM Queuing	54
CPM Filters and Traffic Management	55
TTL Security for LDP	56
Exponential Login Backoff	57
User Lockout	58

Table of Contents

Encryption	59
802.1x Network Access Control	59
TCP Enhanced Authentication Option	59
Packet Formats	60
Keychain	62
Configuration Notes	64
General	64
Configuring Security with CLI	65
Setting Up Security Attributes	66
Configuring Authentication	66
Configuring Authorization	67
Configuring Accounting	69
Security Configurations	70
Configuration Tasks	71
Security Configuration Procedures	72
Configuring Management Access Filters	72
Configuring IP CPM Filters Policy	75
Configuring MAC CPM Filters	76
Configuring CPM Queues	77
IPSec Certificates Parameters	78
Configuring Profiles	80
Configuring Users	81
Configuring Keychains	82
Copying and Overwriting Users and Profiles	83
User	83
Profile	85
RADIUS Configurations	87
Configuring RADIUS Authentication	87
Configuring RADIUS Authorization	88
Configuring RADIUS Accounting	89
Configuring 802.1x RADIUS Policies	90
Configuring CPU Protection Policies	91
TACACS+ Configurations	92
Enabling TACACS+ Authentication	92
Configuring TACACS+ Authorization	93
Configuring TACACS+ Accounting	94
Enabling SSH	95
Configuring Login Controls	96
Security Command Reference	97
Command Hierarchies	97
Configuration Commands	97
Security Commands	98
Login Control Commands	111
Show Commands	112
Login Control	113
Clear Commands	113
Debug Commands	113
Tools Commands	113

SNMP

In This Chapter	281
SNMP Overview	282
SNMP Architecture	282
Management Information Base	282
SNMP Protocol Operations	283
SNMP Versions	283
Management Information Access Control	284
User-Based Security Model Community Strings	285
Views	285
Access Groups	285
Users	287
Per-VRN Logs and SNMP Access	287
Per-SNMP Community Source IP Address Validation	287
Which SNMP Version to Use?	288
Configuration Notes	290
General	290
Configuring SNMP with CLI	291
SNMP Configuration Overview	292
Configuring SNMPv1 and SNMPv2c	292
Configuring SNMPv3	292
Basic SNMP Security Configuration	293
Configuring SNMP Components	294
Configuring a Community String	295
Configuring View Options	295
Configuring Access Options	296
Configuring USM Community Options	297
Configuring Other SNMP Parameters	298
SNMP Command Reference	299
Command Hierarchies	299
Configuration Commands	299

NETCONF

In This Chapter	333
NETCONF Overview	334
NETCONF Introduction	334
NETCONF in SR OS	335
YANG Data Models	336
Transport and Sessions	336
NETCONF Operations	337
Datastores and URLs	340
General NETCONF behavior	341
Establishing a NETCONF Session	351
XML Content Layer	352
<edit-config> with XML Content Layer	353
<get-config> with XML Content Layer	354
XML Content Layer Examples	359
CLI Content Layer	362
CLI Content Layer Examples	363
NETCONF Command Reference	369

Table of Contents

Command Hierarchies	369
Configuration Commands	369
Event and Accounting Logs	
In This Chapter	377
Logging Overview	378
Log Destinations	380
Console	380
Session	380
Memory Logs	380
Log Files	381
SNMP Trap Group	383
Syslog	383
Event Logs	385
Event Sources	386
Event Control	387
Log Manager and Event Logs	389
Event Filter Policies	390
Event Log Entries	391
Simple Logger Event Throttling	393
Default System Log	394
Event Handling System	394
Accounting Logs	396
Accounting Records	396
Accounting Files	412
Design Considerations	412
Reporting and Time-Based Accounting	413
Overhead Reduction in Accounting: Custom Record	414
User Configurable Records	414
Changed Statistics Only	414
Configurable Accounting Records	415
Significant Change Only Reporting	415
Immediate Completion of Records	417
AA Accounting per Forwarding Class	417
Configuration Notes	418
Configuring Logging with CLI	419
Log Configuration Overview	420
Log Types	420
Basic Event Log Configuration	421
Common Configuration Tasks	422
Configuring an Event Log	422
Configuring a File ID	424
Configuring an Accounting Policy	425
Configuring Event Control	426
Configuring Throttle Rate	427
Configuring a Log Filter	428
Configuring an SNMP Trap Group	429
Setting the Replay Parameter	431
Shutdown In-Band Port	433
No Shutdown Port	435

Configuring a Syslog Target	437
Configuring an Accounting Custom Record	438
Log Management Tasks	440
Modifying a Log File	441
Deleting a Log File	443
Modifying a File ID	444
Deleting a File ID	445
Modifying a Syslog ID	446
Deleting a Syslog	446
Modifying an SNMP Trap Group	447
Deleting an SNMP Trap Group	448
Modifying a Log Filter	448
Deleting a Log Filter	450
Modifying Event Control Parameters	450
Returning to the Default Event Control Configuration	451
Log Command Reference	453
Command Hierarchies	453
Standards and Protocol Support	545

Table of Contents

List of Tables

Getting Started

Table 1: Configuration Process	17
--------------------------------------	----

Security

Table 2: Supported Authorization Configurations	29
Table 3: Security Methods Capabilities	34
Table 4: Ranges versus Levels and OpCodes	40
Table 5: CPU Protection and Squelching	43
Table 6: Keychain Mapping	62
Table 7: Security Algorithm Support Per Protocol	63
Table 8: Security Configuration Requirements	71
Table 9: Opcode Values	136
Table 10: IP Protocol Names	200
Table 11: Show System Security Access Group Output Fields	231
Table 12: Show System Security Authentication Output Fields	232
Table 13: Show Communities Output Fields	235
Table 14: Show CPM IP Filter Output Fields	236
Table 15: Show CPM IPv6 Filter Output Fields	238
Table 16: Show Distributed CPU Protection Output Fields	245
Table 17: Show Distributed CPU Protection Policer Output Fields	246
Table 18: Show Distributed CPU Protection Policer Output Fields	250
Table 19: Show Management Access Filter Output Fields	257
Table 20: Show Password Options Output Fields	258
Table 21: Show Per-Peer-Queuing Output Fields	260
Table 22: Show User Profile Output Fields	261
Table 23: Show Source Address Output Fields	262
Table 24: Pass/Fail Login Attempts	268
Table 25: Show View Output Fields	269
Table 26: Show Users Output Fields	272
Table 27: Output Parameters	279

SNMP

Table 28: Counters Output Fields	311
Table 29: Counters Output Fields	312
Table 30: Show System Information Output Fields	313
Table 31: Show System Security Access-Group Output Fields	317
Table 32: Show Community Output Fields	325
Table 33: Show Source Access List Output Fields	326
Table 34: Show SSH Output Fields	327
Table 35: Show User Output Fields	329
Table 36: Show System Security View Output Fields	330

List of Tables

Event and Accounting Logs

Table 37: Event Severity Levels	378
Table 38: Router to Syslog Severity Level Mappings	384
Table 39: Valid Filter Policy Operators	390
Table 40: Log Entry Field Descriptions	391
Table 41: Accounting Record Name and Collection Periods	396
Table 42: Accounting Record Name Details	397
Table 43: Policer Stats Field Descriptions	409
Table 44: Queue Group Record Types	410
Table 45: Queue Group Record Type Fields	410
Table 46: Show Accounting Policy Output Fields	521
Table 47: Accounting Policy Output Fields	523
Table 48: Event Log Filter Summary Output Fields	532
Table 49: Event Log Filter Detail Output Fields	533
Table 50: Log Filter Match Criteria Output Fields	533
Table 51: Show Log-Collector Output Fields	536
Table 52: SNMP Trap Group Output Fields	541
Table 53: Show Log Syslog Output Fields	542

List of Figures

Security

Figure 1: RADIUS Requests and Responses	20
Figure 2: Security Flow	35
Figure 3: Profile Marking	37
Figure 4: ETH-CFM Hierarchical Model	42
Figure 5: Per SAP per Protocol Static Rate Limiting with DCP	46
Figure 6: Per Network Interface per Protocol Static Rate Limiting with DCP	46

SNMP

Figure 7: SNMPv1 and SNMPv2c Configuration and Implementation Flow	289
--------------------------------------------------------------------------	-----

NETCONF

Figure 8: NETCONF RPC Request	334
Figure 9: NETCONF Layers (RFC 6241)	335

Event and Accounting Logs

Figure 10: Event Logging Block Diagram	385
Figure 11: EHS Object Relationships	395

List of Figures

Preface

About This Guide

This guide describes management of SR OS routers including access to the router (AAA, CLI, SNMP), basic router security, logs, notifications and facility alarms.

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

Audience

This guide is intended for network administrators who are responsible for configuring the 7450 ESS routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Concepts described in this guide include the following:

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

List of Technical Publications

The 7450 ESS documentation set is composed of the following guides:

- **7450 ESS Basic System Configuration Guide**
This guide describes basic system configurations and operations.
- **7450 ESS System Management Guide**
This guide describes system security and access configurations as well as event logging and accounting logs.
- **7450 ESS Interface Configuration Guide**
This guide describes card, Media Dependent Adapter (MDA) and port provisioning.
- **7450 ESS Router Configuration Guide**
This guide describes logical IP routing interfaces and associated attributes such as an IP address, as well as IP and MAC-based filtering, and VRRP and Cflowd.
- **7450 ESS Routing Protocols Guide**
This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, BGP, and route policies.
- **7450 ESS MPLS Guide**
This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- **7450 ESS Services Overview Guide**
This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.
- **7450 ESS Layer 2 Services and EVPN Guide**
This guide describes Virtual Leased Lines (VLL), Virtual Private LAN Service (VPLS), Provider Backbone Bridging (PBB), and Ethernet VPN (EVPN).
- **7450 ESS Layer 3 Services Guide**
This guide describes Internet Enhanced Services (IES) and Virtual Private Routed Network (VPRN) services.
- **7450 ESS Versatile Service Module Guide**
This guide describes how to configure service parameters for the Versatile Service Module (VSM).
- **7450 ESS OAM and Diagnostics Guide**
This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- **7450 ESS Triple Play Guide**

This guide describes Triple Play services and support provided by the 7450 ESS and presents examples to configure and implement various protocols and services.

- 7450 ESS Quality of Service Guide

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

- Multi-Service Integrated Service Adapter Guide

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

Technical Support

If you purchased a service agreement for your 7450 ESS 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, follow this link to contact an Alcatel-Lucent support representative and to access product manuals and documentation updates:

<http://support.alcatel-lucent.com>

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 7450 ESS 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 281
Secure network management	Configure NETCONF elements.	NETCONF on page 333
Operational functions	Configure event and accounting logs.	Event and Accounting Logs on page 377
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 545

Note: In SR OS 12.0.R4 any function that displays an IPv6 address or prefix changes to reflect rules described in RFC 5952, *A Recommendation for IPv6 Address Text Representation*. Specifically, hexadecimal letters in IPv6 addresses are now represented in lowercase, and the correct compression of all leading zeros is displayed. This changes visible display output compared to previous SR OS releases. Previous SR OS behavior can cause issues with operator scripts that use standard IPv6 address expressions and with libraries that have standard IPv6 parsing as per RFC 5952 rules. See the section on IPv6 Addresses in the Router Configuration Guide for more information.

In This Chapter

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

- [Authentication, Authorization, and Accounting on page 20](#)
 - [Authentication on page 21](#)
 - [Authorization on page 28](#)
 - [Accounting on page 32](#)
- [Security Controls on page 34](#)
 - [When a Server Does Not Respond on page 34](#)
 - [Access Request Flow on page 35](#)
- [CPU Protection on page 36](#)
- [Vendor-Specific Attributes \(VSAs\) on page 51](#)
- [Other Security Features on page 52](#)
 - [Per Peer CPM Queuing on page 54](#)
 - [CPM Filters and Traffic Management on page 55](#)
 - [Secure Shell \(SSH\) on page 52](#)
 - [Encryption on page 59](#)
 - [802.1x Network Access Control on page 59](#)
- [Configuration Notes on page 64](#)

Authentication, Authorization, and Accounting

This chapter describes authentication, authorization, and accounting (AAA) used to monitor and control network access on 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 routers to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, or FTP. You can select the authentication order which determines the authentication method to try first, second, and third.

The router 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.

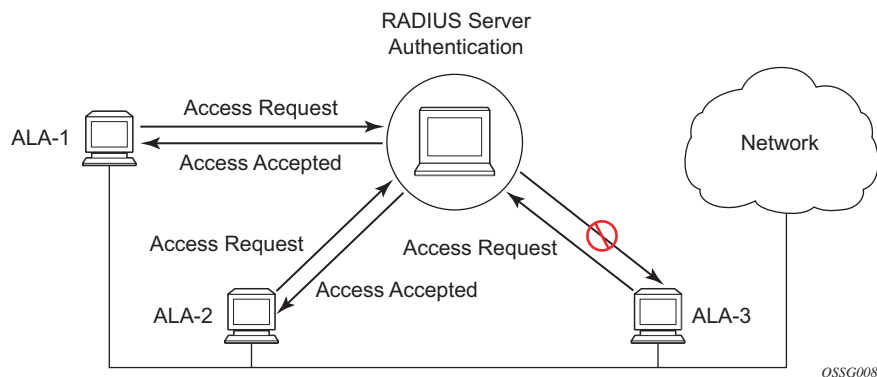


Figure 1: RADIUS Requests and Responses

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 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 routers does not require the configuration of VSAs (Vendor Specific Attributes) on the RADIUS server. However, users, user access permissions, and command authorization profiles must be configured on each router.

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

- [Local Authentication on page 22](#)
- [RADIUS Authentication on page 22](#)
- [TACACS+ Authentication on page 27](#)

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

RADIUS Authentication

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

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

RADIUS Server Selection

The RADIUS server selection algorithm is used by different applications:

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

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

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

Direct Mode

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

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

Round-Robin Mode

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

Server Reachability Detection

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

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

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

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

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

Application Specific Behavior

Operator Management

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

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

RADIUS Authentication

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

RADIUS Challenge/Response Interactive Authentication

Challenge-response interactive authentication is used for key authentication where the Radius server is asking for the valid response to a displayed challenge. The challenge packet includes a challenge to be displayed to the user, such as a unique generated numeric value unlikely ever to be repeated. Typically this is obtained from an external server that knows what type of authenticator is in the possession of the authorized user and can therefore choose a random or non-repeating pseudorandom number of appropriate length.

The user then enters the challenge into his device (or software) and it calculates a response, which the user enters into the client which forwards it to the RADIUS server via an access request. If the response matches the expected response, the RADIUS server allows the user access, otherwise it rejects the response.

RADIUS challenge/response mode is enabled using the CLI interactive-authentication command in the config>system>security>radius context. RADIUS interactive authentication is disabled by default. The option needs to be enabled via CLI.

Enabling interactive authentication under CLI does not mean that the system uses RADIUS challenge/response mode by default. The configured password authentication-order parameter is used. If the authentication-order parameter is local RADIUS, the system will first attempt to

login the user via local authentication. If this fails, the system will revert to RADIUS and challenge/response mode. The authentication-order will precede the RADIUS interactive-authentication mode.

Even if the authentication-order is RADIUS local, the standard password prompt is always displayed. The user enters a username and password at this prompt. If RADIUS interactive-authentication is enabled the password does not have to be the correct password since authentication is accomplished using the RADIUS challenge/response method. The user can enter any password. The username and password are sent to the RADIUS server, which responds with a challenge request that is transmitted back to the node by the RADIUS server. Once the user enters the challenge response, the response is authenticated by the RADIUS server to allow node access to the user.

For example, if the system is configured with system security authentication-order set to local RADIUS, at the login prompt the user can enter the username "admin" and the corresponding password. If the password for local authentication does not match, the system falls into RADIUS authentication mode. The system checks the interactive-authentication configuration and if it is enabled it enters into challenge/response mode. It sends the username and password to the RADIUS server, and the server sends the challenge request back to the node and to the user where it appears as a challenge prompt onscreen. A challenge received from the RADIUS server typically contains a string and a hardware token that can be used to generate a password on the users' local personal token generator. For example, the RADIUS server might send the challenge prompt "Enter response for challenge 12345:" to SR OS. The string "12345" can be entered in the local token generator which generates the appropriate challenge response for the entered string. This challenge response can then be entered on the SR-OS prompt for authorization.

Once the user enters the correct challenge response it is authenticated via the RADIUS server. The server authenticates the user and the user gains access to the node.

If session timeout and Idle timeout values are configured on the RADIUS server, these are used to govern the length of time before SR-OS cancels the challenge prompt. If the user is idle longer than the received idle-timeout (seconds) from the RADIUS server, and/or if the user does not press ENTER before the received session-timeout (seconds).

Note: For SSH only the session-timeout value is used. The SSH stack cannot track character input into the login prompt until the enter key is pressed.

Note: If the idle/session attribute is not available or if the value is set to a very large number, SR OS uses the smallest value set in "configure system login-control idle-timeout" and the idle/session timeout attribute value to terminate the prompt. If the "login-control idle-timeout" is set to 0 (equivalent to infinite), the maximum idle-timeout (24-hours) is used for the calculation.

SR-OS displays the log-in attempts/failure per user in the "show system security user user-name" screen. If the RADIUS rejects a challenge response, it counts as a failed login attempt and a new prompt is displayed. The number of failed attempts is limited by the value set for "configure

Authentication

system security password attempt.” An incorrect challenge response results in a failure count against the password attempts.

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

SR OS routers support local, RADIUS, and TACACS+ authorization to control the actions of specific users. Any combination of these authorization methods can be configured to control actions of specific users:

- [Local Authorization on page 28](#)
- [RADIUS Authorization on page 28](#)
- [TACACS+ Authorization on page 29](#)

Local authorization and RADIUS authorization operate 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 51](#).

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, such as TACACS+ or RADIUS authorization.

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.

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

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

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

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

Table 2 displays the following scenarios:

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

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

Table 2: Supported Authorization Configurations

	Router	RADIUS Supplied Profile
Routerconfigured 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.

TACACS+ Authorization

TACACS+ authorization operates in one of three ways:

- All users who authenticate via TACACS+ can use a single common default profile that is configured on the SR OS Router, or
- Each command attempted by a user is sent to the TACACS+ server for authorization

- The operator can configure local profiles and map **tacplus priv-lvl** based authorization to those profiles (the **use-priv-lvl** option)

To use a single common default profile to control command authorization for TACACS+ users, the operator must configure the **tacplus use-default-template** option and configure the parameters in the **tacplus_default user-template** to point to a valid local profile.

If the default template is not being used for TACACS+ authorization and the **use-priv-lvl** option is not configured, then each CLI command issued by an operator is sent to the TACACS+ server for authorization. The authorization request sent by SR OS contains the first word of the CLI command as the value for the TACACS+ **cmd** and all following words become a **cmd-arg**. Quoted values are expanded so that the quotation marks are stripped off and the enclosed value are seen as one **cmd** or **cmd-arg**.

Examples

Here is a set of examples, where the following commands are typed in the CLI:

- "show"
- "show router"
- "show port 1/1/1"
- "configure port 1/1/1 description "my port"

This results in the following AVPairs:

cmd=show

cmd=show
cmd-arg=router

cmd=show
cmd-arg=port
cmd-arg=1/1/1

cmd=configure
cmd-arg=port
cmd-arg=1/1/1
cmd-arg=description
cmd-arg=my port

For TACACS+ authorization, SR OS sends the entire CLI context in the **cmd** and **cmd-arg** values. Here is a set of examples where the CLI context is different:

- *A:dut-c# configure service
- *A:dut-c>config>service# vprn 555 customer 1 create
- *A:dut-c>config>service>vprn\$ shutdown

This results in the following AVPairs:

```
cmd =configure
cmd-arg=service
```

```
cmd=configure
cmd-arg=service
cmd-arg=vprn
cmd-arg="555"
cmd-arg=customer
cmd-arg=1
cmd-arg=create
```

```
cmd=configure
cmd-arg=service
cmd-arg=vprn
cmd-arg="555"
cmd-arg=customer
cmd-arg=1
cmd-arg=create
cmd-arg=shutdown
```

Accounting

When enabled, RADIUS accounting sends command line accounting from the router to the RADIUS server. The router sends spar

s using UDP packets at port 1813 (decimal).

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

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

RADIUS Accounting

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

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

TACACS+ Accounting

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

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

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

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

Security Controls

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

Table 3: Security Methods Capabilities

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

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

When a Server Does Not Respond

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

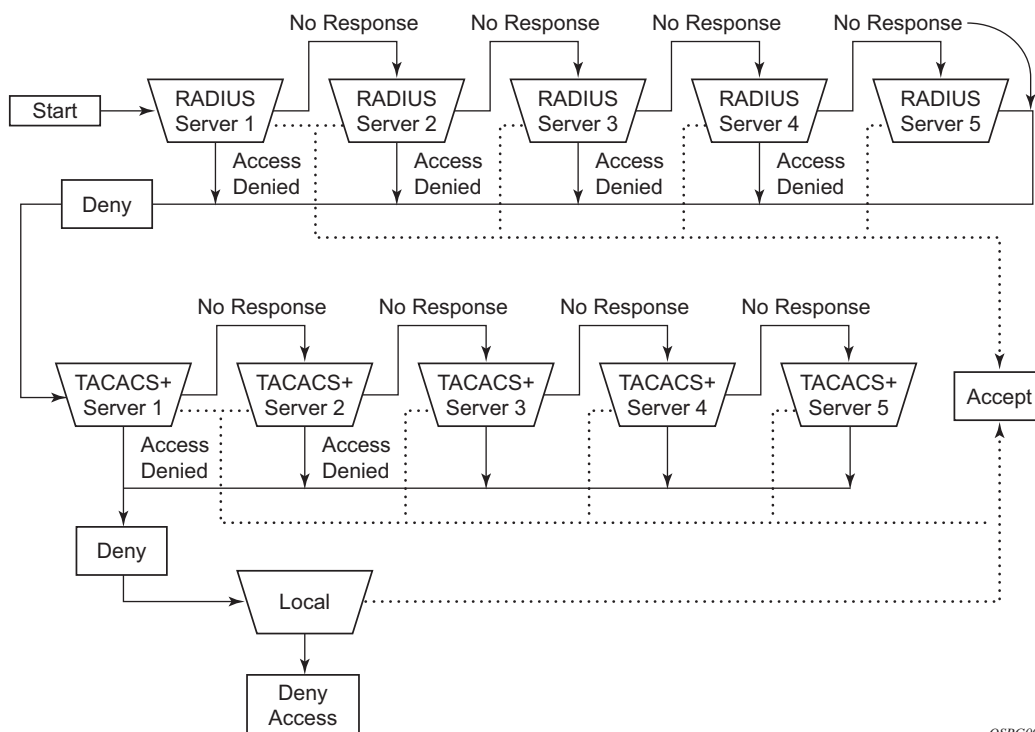
Periodic checks to determine if the primary server is responsive again are not performed. If a server is down, it will not be contacted for 5 minutes. If a login is attempted after 5 minutes, then the server is contacted again. When a server does not respond with the health check feature enabled, the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

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

Access Request Flow

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

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



OSRG009

Figure 2: Security Flow

CPU Protection

SR OS provides several rate limiting mechanisms to protect the CPM/CFM processing resources of the router:

- CPU Protection: A centralized rate limiting function that operates on the CPM to limit traffic destined to the CPUs.
- Distributed CPU Protection: A control traffic rate limiting protection mechanism for the CPM/CFM that operates on the line cards (hence ‘distributed’).

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 protocols LACP (ethernet LAG control) and LMI (ATM, Ethernet and Frame Relay). The rate is a per-link limit (each link in the system will have LACP/LMI 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 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 — Used to limit the control traffic destined to the CPM from each individual source. This per-source-rate is only applied when an object (SAP) is configured with a `cpu-protection` policy and also with the optional `mac-monitoring` or `ip-src-monitoring` keywords. A source is defined as a *SAP, Source MAC Address* tuple for `mac-monitoring` and as a *SAP, Source IP Address* tuples for **ip-src-monitoring**. Only certain protocols (as configured under *included-protocols* in the `cpu` protection policy) are limited (per source) when the **ip-src-monitoring** keyword is used.
- 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.

Protocols controlled by the protocol-protection mechanism include:

- OSPFv2
- OSPFv3
- IS-IS
- RSVP-TE
- RIP
- PIM
- MLD
- IGMP
- 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
- 7950 XRS

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 though 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.

ETH-CFM Ingress Squelching

CPU protection provides a granular method to control which ETH-CFM packets are processed. As indicated in the previous section, a unique rate can be applied to ETH-CFM packets classifying on specific MD-Level and specific OpCode and applied to both ingress (Down MEP and ingress MIP) and egress (Up MEP and egress MIP) extraction. That function is to protect the CPU upon extraction when a Management Point (MP) is configured.

It is also important to protect the ETH-CFM architecture deployed in the service provider network. The protection scheme here varies from CPU protection. This model is used to prevent ETH-CFM frames at the service provider MD-levels from gaining access to the network even when extraction is not in place. ETH-CFM squelching allows the operator to achieve this goal using a simple method to drop all ETH-CFM packets at or below the configured MD-level. The ETH-CFM squelch feature is ingress only.

Figure 4 shows a typical ETH-CFM hierarchical model with a Subscriber ME (6), Test ME (5), EVC ME (4) and an Operator ME (2). This model provides the necessary transparency at the different levels of the architecture. For security reasons, it may be necessary to prevent errant levels from entering the service provider network at the UNI, ENNI, or other untrusted interconnection points. Configuring squelching at level four on both UNI-N interconnection ensures that ETH-CFM packets matching the SAP or binding delimited configuration will silently discard ETH-CFM packets at ingress.

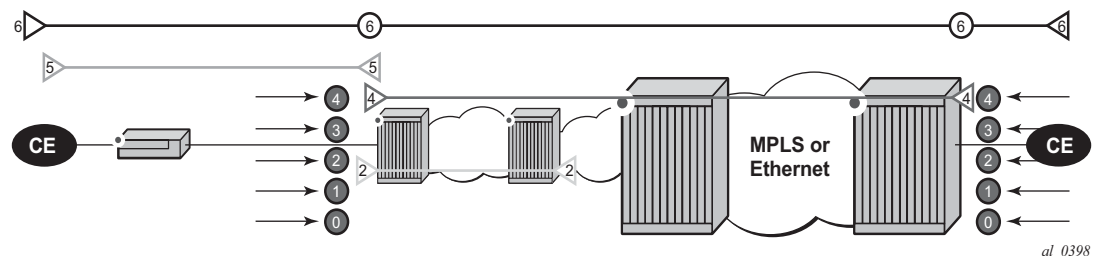


Figure 4: ETH-CFM Hierarchical Model

Squelching configuration uses a single MD-level [0..7] to silently drop all ETH-CFM packets matching the SAP or binding delimited configuration at and below the specified MD-level. In Figure 4, a squelch level is configured at MD-level 4. This means the configuration will silently discard MD-levels 0,1,2,3 and 4, assuming there is a SAP or binding match.

Note: Extreme caution must be used when deploying this feature.

The operator is able to configure Down MEPs and ingress MIPs that conflict with the squelched levels. This also means that any existing MEP or MIP processing ingress CFM packets on a SAP on Binding where a squelching policy is configured will be interrupted as

soon as this command is entered into the configuration. These MPs will not be able to receive any ingress ETH-CFM frames because squelching is processed before ETH-CFM extraction.

CPU Protection Extensions for ETH-CFM are still required in the model above because the Subscriber ME (6) and the Test ME (5) are entering the network across an untrusted connection, the UNI. ETH-CFM squelching and CPU Protection for ETH-CFM can be configured on the same SAP or binding. Squelching is first in the process order followed by CPU Protection for ETH-CFM.

MPs configured to support primary VLAN are not subjected to the squelch function. Primary VLAN based MPs, supported only on Ethernet SAPs, are extractions that take into consideration an additional VLAN beyond the SAP configuration.

The difference in the two protection mechanisms is shown in the [Table 5](#). CPU Protection is used to control access to the CPU resources when processing is required. Squelching is required when the operator is protecting the ETH-CFM architecture from external sources.

Table 5: CPU Protection and Squelching

Description	CPU Protection Extension for ETH-CFM	ETH-CFM Squelching
Ingress Filtering	Yes	Yes
Egress Filtering	Yes	No
Granularity	Specified Level AND OpCode	Level (At and below)
Rate	Configurable Rate (includes 0=drop all)	Silent Drop
Primary VLAN Support	Rate shared with SAP delineation	Not exposed to squelch
Extraction	Requires MEP or MIP to extract	No MEP or MIP required

As well as including the squelching information under the **show service *service-id* all**, display output the **squelch-ingress-level** key has been added to the **sap-using** and **sdp-using show** commands.

```
show service sap-using squelch-ingress-levels
=====
ETH-CFM Squelching
=====
PortId          SvcId          Squelch Level
-----
6/1/1:100.*      1              0 1 2 3 4 5 6 7
```

ETH-CFM Ingress Squelching

```
lag-1:100.*      1      0 1 2 3 4
6/1/1:200.*      2      0 1 2
lag-1:200.*      2      0 1 2 3 4 5
-----
Number of SAPs: 4
-----
=====
show service sdp-using squelch-ingress-levels
=====
ETH-CFM Squelching
=====
SdpId           SvcId           Type Far End           Squelch Level
-----
12345:4000000000 2147483650     Spok 1.1.1.1           0 1 2 3 4
=====
```

Extreme caution must be used when deploying this feature.

Distributed CPU Protection (DCP)

SR OS provides several rate limiting mechanisms to protect the CPM/CFM processing resources of the router:

- **CPU Protection:** A centralized rate limiting function that operates on the CPM to limit traffic destined to the CPUs. This feature is described elsewhere in this guide.
- **Distributed CPU Protection:** A control traffic rate limiting protection mechanism for the CPM/CFM that operates on the line cards (hence 'distributed').

Distributed CPU Protection (DCP) offers a powerful per-protocol-per-object (examples of objects are SAPs and network interfaces) rate limiting function for control protocol traffic that is extracted from the data path and sent to the CPM. The DCP function is implemented on the router line cards that allows for high levels of scaling and granularity of control.

The DCP rate limiting is configured via policies that are applied to objects (for example, SAPs).

The basic types of policers in DCP are:

- **Enforcement Policers** — An instance of a policer that is policing a flow of packets comprised of a single (or small set of) protocols(s) arriving on a single object (for example, SAP). Enforcement policers perform a configurable action (for example, discard) on packets that exceed configured rate parameters. There are two basic sub-types of enforcement policers:
 - **Static policers** — always instantiate.
 - **Dynamic policers** — only instantiated (allocated from a free pool of dynamic policers) when a local monitor detects non-conformance for a set of protocols on a specific object.
- **Local Monitors** — A policer that is primarily used to measure the conformance of a flow comprised of multiple protocols arriving on a single object. Local monitors are used as a trigger to instantiate dynamic policers.

The use of dynamic policers reduces the number of policers required to effectively monitor and control a set of protocols across a large set of objects since the per-protocol-per-object dynamic policers are only instantiated when an attack or misconfiguration occurs, and they are only instantiated for the affected objects.

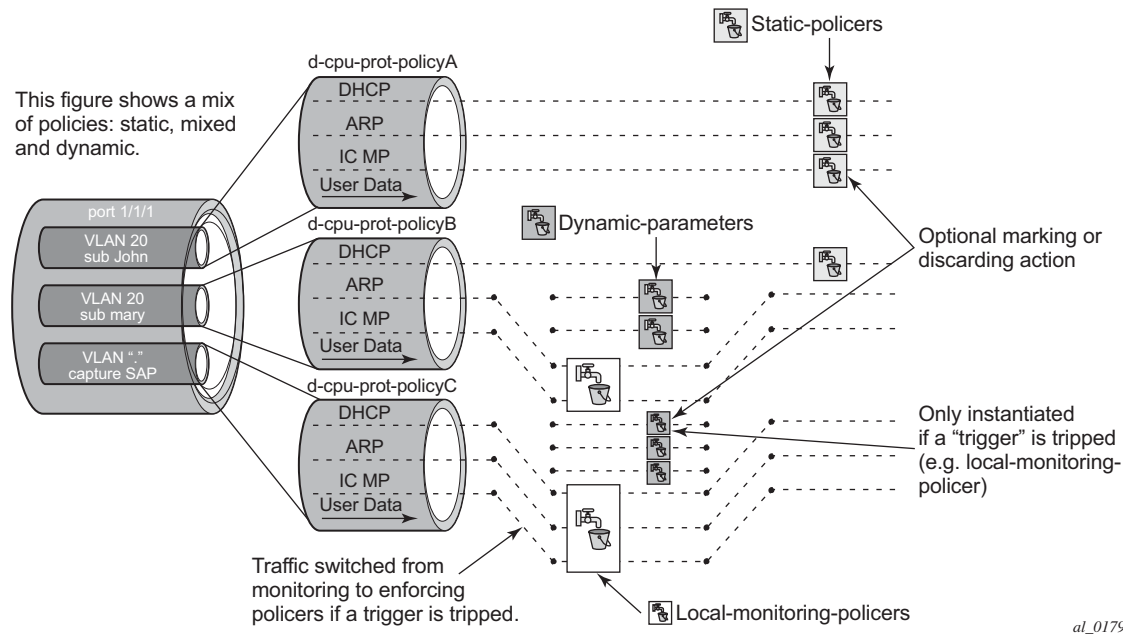


Figure 5: Per SAP per Protocol Static Rate Limiting with DCP

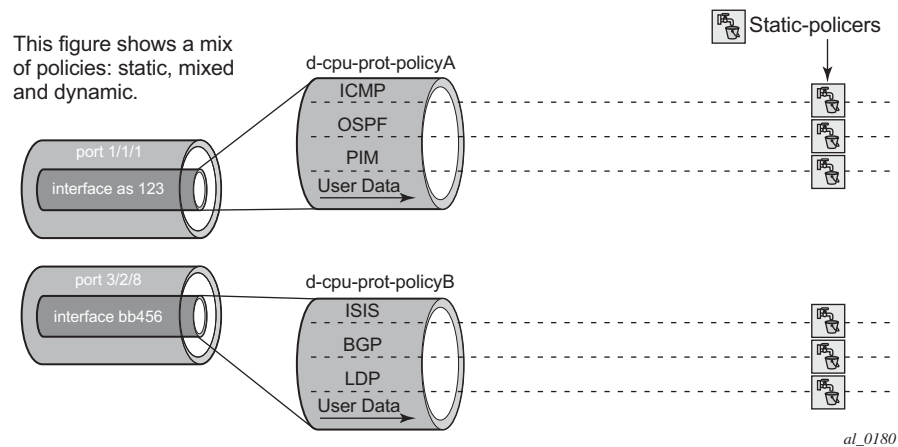


Figure 6: Per Network Interface per Protocol Static Rate Limiting with DCP

Applicability of Distributed CPU Protection

dist-cpu-protection (DCP) policies can be applicable to the following types of objects:

- most types of SAPs, including capture SAPs and SAPs on pseudo wires, but it is not applicable to b-vpls saps (b-saps).
- Network Interfaces, but not to any other type of interface. A DCP policy can be configured at the interface sap instead.

Control packets that are both forwarded (which means they could be subject to normal QoS policy policing) and also copied for extraction are not subject to Distributed CPU Protection (including in the all-unspecified bucket). This includes traffic snooping (for example, PIM in VPLS) as well as control traffic that is flooded in an R-VPLS instance and also extracted to the CPM such as ARP, ISIS and VRRP. Centralized per SAP/interface cpu-protection can be employed to rate limit or mark this traffic if desired.

Control traffic that arrives on a network interface, but inside a tunnel (for example, SDP, LSP, PW) and logically terminates on a service (that is, traffic that is logically extracted by the service rather than the network interface layer itself) will bypass the DCP function. The control packets in this case will not be subject to the DCP policy that is assigned to the network interface on which the packets arrived. This helps to avoid customer traffic in a service from impacting other services or the operator's infrastructure.

Control packets that are extracted in a vprn service, where the packets arrived into the node via a vpls SAP (that is, r-vpls scenario), will use the DCP policy and policer instances associated with the vpls SAP. In this case the DCP policy that an operator creates for use on VPLS SAPs, for VPLSs that have a l3-interface bound to them (r-vpls), may have protocols like OSPF, ARP, configured in the policy.

Log Events, Statistics, Status and SNMP support

A comprehensive set of log events are supported for DCP in order to alert the operator to potential attacks or misconfigurations and to allow tuning of the DCP settings. Refer to the NOTIFICATION-TYPE objects with “Dcp” in the names in the following MIBs for details:

- TIMETRA-CHASSIS-MIB
- TIMETRA-SAP-MIB
- TIMETRA-VRTR-MIB

The log events can also be seen in the CLI using the following **show log event-control | match Dcp** command

DCP throttles the rate of DCP events to avoid event floods when multiple parallel attacks or problems are occurring.

Many of the DCP log events can be individually enabled or disabled at the DCP policy level (in the DCP policy config) as well as globally in the system (in log event-control).

If needed when a DCP log event indicates a SAP, and that SAP is an MSAP, the operator can determine which subscriber(s) is/are on a specific MSAP by using the **show service active-subs** command and then filtering (“| match”) on the msap string.

Statistics and status related to DCP are available both via:

- CLI
- SNMP — See various tables and objects with “Dcp” or “DCpuProt” in their name in the TIMETRA-CHASSIS-MIB, TIMETRA-SECURITY-MIB, TIMETRA-SAP-MIB and TIMETRA-VRTR-MIB

DCP Policer Resource Management

The policer instances are a limited h/w resource on a given forwarding plane. DCP policers (static, dynamic, local-monitor) are consumed from the overall forwarding plane policer resources (from the ingress resources if ingress and egress are partitioned). Each per-protocol policer instantiated reduces the number of FP child policers available for other purposes.

When DCP is configured with dynamic enforcement, then the operator must set aside a pool of policers that can be instantiated as dynamic enforcement policers. The number of policers reserved for this function are configurable per card/fp. The policers in this pool are not available for other purposes (normal SLA enforcement).

Static enforcement policers and local monitoring policers use policers from the normal/global policer pool on the card/fp. Once a static policer is configured in a DCP policy and it is referenced by a protocol in the policy, then this policer will be instantiated for each object (SAP or network interface) that is created and references the policy. If there is no policer free on the associated card/fp, then the object will be blocked from being created. Similarly for local monitors: once a local monitoring policer is configured and referenced by a protocol, then this policer will be instantiated for each object that is created and references the policy. If there is no policer free, then the object will be blocked from being created.

Dynamic enforcement policers are allocated as needed (when the local monitor detects non-conformance) from the reserved dynamic-enforcement-policer-pool.

When a DCP policy is applied to an object on a LAG, then a set of policers is allocated on each forwarding plane (on each line card that contains a member of the LAG). The LAG mode is ignored and the policers are always shared by all ports in the LAG on that forwarding plane on the SAP/interface. In other words, with link-mode lag a set of DCP policers are not allocated per port in the LAG on the SAP.

In order to support large scale operation of DCP, and also to avoid overload conditions, a polling process is used to monitor state changes in the policers. This means there can be a delay between when an event occurs in the data plane and when the relevant state change or event notification occurs towards an operator, but in the meantime the policers are still operating and protecting the control plane.

Operational Guidelines and Tips

The following points offer various optional guidelines that may help an operator decide how to leverage Distributed CPU Protection.

- The rates in a policy assigned to a capture SAP should be higher than those assigned to MSAPs that will contain a single subscriber. The rates for the capture sap policy should allow for a burst of MSAP setups.
- To completely block a set of specific protocols on a given SAP, create a single static policer with a rate of 0 and map the protocols to that policer. Dynamic policers and local monitors can't be used to simultaneously allow some protocols but block others (the non-zero rates in the monitor would let all protocols slip through at a low rate).
- During normal operation it is recommended to configure "log-events" (no verbose keyword) for all static-policers, in the dynamic-parameters of all protocols and for all local-monitoring-policers. The verbose keyword can be used selectively during debug, testing, tuning and investigations.
- Packet based rate limiting is generally recommended for low rate subscriber based protocols whereas kbps rate limiting is recommended for higher rate infrastructure protocols (such as BGP).
- It is recommended to configure an exceed-action of low-priority for routing and infrastructure protocols. Marked packets are more likely to be discarded if there is congestion in the control plane of the router, but will get processed if there is no contention for CPU resources allowing for a work-conserving behavior in the CPM.
- In order to assign a different dist-cpu-protection policy to a specific MSAP (instance) or to all MSAPs for a specific msap policy, the operator can assign a new dist-cpu-protection policy to the MSAP policy and then use the **eval-msap** tool:

```
A:nodeA>tools>perform# subscriber-mgmt eval-msap  
- eval-msap { policy <msap-policy-name> | msap <sap-id> }
```

Note that any new MSAPs will also be assigned the new dist-cpu-protection policy.

- If needed, an operator can determine which subscriber is on a specific MSAP by using the **show service active-subs** command and then filtering ("| match") on the msap string.
- If protocol X is trusted, and using the "all-unspecified" protocol is not required, then simply avoid creating protocol X in the policy configuration.
- If protocol X is trusted, but the all-unspecified bucket is required, then there are two options:
 - avoid creating protocol X so that it is treated as part of the all-unspecified bucket (but account for the packets from X in the all-unspecified rate and local-mon rate),
 - or
 - create protocol X and configure it to bypass.

Vendor-Specific Attributes (VSAs)

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

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

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

- `timetra-access <ftp> <console> <both>` — This is a mandatory command that must be configured. This command specifies if the user has FTP and /or console (serial port, Telnet, and SSH) access.
- `timetra-profile <profile-name>` — When configuring this VSA for a user, it is assumed that the user profiles are configured on the local router and the following applies for local and remote authentication:
 1. The `authentication-order` parameters configured on the router must include the `local` 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 place by one of the configured authentication methods (local, RADIUS, or TACACS+). With authentication and encryption, SSH allows for a secure connection over an insecure network.

The OS 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.

The 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 “cfl:\dir1\file1” will be transmitted to the SCP server as “cfl: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.

Two cipher lists, the client-cipher-list and the server-cipher-list, can be configured for negotiation of the best compatible ciphers between the the client and server. The two cipher lists can be created and managed under the security ssh sub menu. The client-cipher-list is used when SR OS is acting as ssh client and the server-cipher-list is used when the SR OS is acting as a server. The first cipher matched on the lists between the client and server is the preferred cipher for the session.

SSH PKI Authentication

The SR OS supports Secure Shell Version 2, but user authentication appears to be limited to using a username and password.

SSH also supports public key authentication whereby the client can provide a signed message that has been encrypted by his private key. As long as the server has been previously configured to know the client's public key, the server can authenticate the client.

Using Public Key authentication (also known as Public Key Infrastructure - PKI) can be more secure than the existing username/password method for a few reasons:

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

This feature includes server side support for SSHv2 public key authentication. It does not include a key generation utility.

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

Key Generation

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

SSHv2 supports both RSA and DSA keys. The Digital Signature Algorithm is a U.S Federal Government standard for digital signatures. PuTTYGen can be used to generate either type of key. The SR OS currently supports only RSA keys.

Assume the client is using PuTTY. First the user generates a key pair using PuTTYgen. The user sets the key type (SSH-1 RSA, SS-2 RSA, or SSH-2 DSA) and sets the number of bits to be used for the key (default = 1024). The user can also configure a passphrase that will be used to store the key locally in encrypted form. If the passphrase is configured the user must enter the passphrase in order to use the private key. Thus, it is a password for the private key. If the passphrase is not used the key is stored in plaintext locally.

Next the user must configure the server to use his public key. This typically requires the user to add the public key to a file on the server. For example, if the server is using OpenSSH, the key must be added to the `ssh/authorized_keys` file. On the SR OS, the user can program the public Key via Telnet/SSH or SNMP.

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 7450 ESS-6/7/12 platforms. It is not supported on the 7450 ESS-1.

CPM Filters and Traffic Management

Alcatel-Lucent routers have traffic management and queuing hardware dedicated to protecting the control plane.

CPM/CFM filters are supported on the following platforms: 7950 XRS, 7750 SR-7/SR-12/SR-c12, and 7710 SR-c4/SR-c12. The filters can be used to drop or accept packets, as well as allocate dedicated hardware shaping (CPM) 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. CPM queueing is supported on the following platforms: 7950 XRS, 7750 SR-7/SR-12, and 7750 SR-c12 (not 7750 SR-1). CPM filters and CPM queueing are supported on 7450 ESS-6/ESS-7/ESS-12 (not ESS-1).

CPM filters and queues control all traffic going in to the CPM from IOMs/XMAs, including all routing protocols. CPM filters 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. CPM filters and queues are not configurable on one-slot chassis.

There are three filters that can be configured as part of the CPM filter policy: IP (v4) filter, IPv6 filter and MAC filter.

The SROS filter 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 of an IP(v4), IPv6, MAC CPM filters must have at least one match criteria defined to be active. A default action can be specified for CPM filter policy that applies to each of IP, IPv6, MAC filters that are in a **no shutdown** state as long as the CPM filter policy has at least one active filter entry in any of the IP(v4), IPv6, and MAC filters.

TTL Security for LDP

The TTL Security Hack (BTSH) was originally designed to protect the 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 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.

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 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 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 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 96](#). The commands are described in [Login, Telnet, SSH and FTP Commands on page 122](#).

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. The list of users who are currently locked-out can be displayed with *show system security user lockout*.

A lock-out for a specific user can be administratively cleared using the *admin user x clear-lockout*.

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 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.

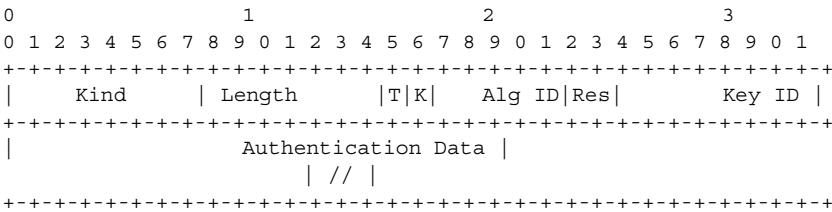
TCP Enhanced Authentication Option

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



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

The keychain mechanism allows for the creation of keys used to authenticate protocol communications. Each keychain entry defines the authentication attributes to be used in authenticating protocol messages from remote peers or neighbors, and it must include at least one key entry to be valid. Through the use of the keychain mechanism, authentication keys can be changed without affecting the state of the associated protocol adjacencies for OSPF, IS-IS, BGP, LDP, and RSVP-TE.

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

- key identifier
- authentication algorithm
- authentication key
- direction
- start time

In addition, additional attributes can be optionally specified, including:

- end time
- tolerance

Table 6 shows the mapping between these attributes and the CLI command to set them.

Table 6: Keychain Mapping

Definition	CLI
The key identifier expressed as an integer (0...63)	<pre>config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry</pre>
Authentication algorithm to use with key[i]	<pre>config>system>security>keychain>direction>bi>entry with algorithm <i>algorithm</i> parameter. config>system>security>keychain>direction>uni>receive>entry with algorithm <i>algorithm</i> parameter. config>system>security>keychain>direction>uni>send>entry with algorithm <i>algorithm</i> parameter.</pre>
Shared secret to use with key[i].	<pre>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</pre>

Table 6: Keychain Mapping (Continued)

Definition	CLI
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
Start time from which key[i] can be used.	config>system>security>keychain>direction>bi>entry>begin-time config>system>security>keychain>direction>uni>send>entry >begin-time
End time after which key[i] cannot be used by sending TCPs.	Inferred by the begin-time of the next key (youngest key rule).
Start time from which key[i] can be used.	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
End time after which key[i] cannot be used	config>system>security>keychain>direction>uni>receive>entry>end-time

The following table details which authentication algorithm can be used in association with specific routing protocols.

[Table 6](#) shows the mapping between these attributes and the CLI command to set them.

Table 7: Security Algorithm Support Per Protocol

Protocol	Clear Text	MD5	HMAC-MD5	HMAC-SHA-1-96	HMAC-SHA-1	HMAC-SHA-256	AES-128-CMAC-96
OSPF	Yes	Yes	No	Yes	Yes	Yes	No
IS-IS	Yes	No	Yes	No	Yes	Yes	No
RSVP	Yes	No	Yes	No	Yes	No	No
BGP	No	Yes	No	Yes	No	No	Yes
LDP	No	Yes	No	Yes	No	No	Yes

Configuration Notes

This section describes security configuration caveats.

General

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

Configuring Security with CLI

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

Topics in this section include:

- [Setting Up Security Attributes on page 66](#)
 - [Configuring Authorization on page 67](#)
 - [Configuring Authorization on page 67](#)
 - [Configuring Accounting on page 69](#)
- [Configuration Tasks on page 71](#)
- [Security Configuration Procedures on page 72](#)
 - [Configuring Management Access Filters on page 72](#)
 - [Configuring IP CPM Filters Policy on page 75](#)
 - [Configuring MAC CPM Filters on page 76](#)
 - [Configuring CPM Queues on page 77](#)
 - [Configuring Profiles on page 80](#)
 - [Configuring Users on page 81](#)
 - [Copying and Overwriting Users and Profiles on page 83](#)
 - [Enabling SSH on page 95](#)
 - [Configuring Login Controls on page 96](#)
 - [RADIUS Configurations on page 87](#)
 - [Configuring RADIUS Authentication on page 87](#)
 - [Configuring RADIUS Authorization on page 88](#)
 - [Configuring RADIUS Accounting on page 89](#)
 - [TACACS+ Configurations on page 92](#)
 - [Enabling TACACS+ Authentication on page 92](#)
 - [Configuring TACACS+ Authorization on page 93](#)
 - [Configuring TACACS+ Accounting on page 94](#)
 - [Configuring 802.1x RADIUS Policies on page 90](#)
 - [Configuring Login Controls on page 96](#)

Setting Up Security Attributes

Configuring Authentication

Refer to the following sections to configure authentication:

- Local authentication
 - [Configuring Profiles on page 80](#)
 - [Configuring Users on page 81](#)
- RADIUS authentication (only)

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

 - [Configuring Profiles on page 80](#)
 - [Configuring RADIUS Authentication on page 87](#)
 - [Configuring Users on page 81](#)
- RADIUS authentication

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

 - [Configuring RADIUS Authentication on page 87](#)
 - [Configuring RADIUS Authorization on page 88](#)
- TACACS+ authentication

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

 - [Configuring Profiles on page 80](#)
 - [Configuring Users on page 81](#)
 - [Enabling TACACS+ Authentication on page 92](#)

Configuring Authorization

Refer to the following sections to configure authorization.

- Local authorization

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

→ [Configuring Profiles on page 80](#)

→ [Configuring Users on page 81](#)

- RADIUS authorization (only)

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

→ [Configuring RADIUS Authorization on page 88](#)

→ [Configuring Profiles on page 80](#)

For RADIUS authorization, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 51](#).

- RADIUS authorization

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

→ [Configuring RADIUS Authorization on page 88](#)

For RADIUS authorization, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 51](#).

→ [Configuring RADIUS Authentication on page 87](#)

→ [Configuring Profiles on page 80](#)

- TACACS+ authorization (only)

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

→ [Configuring TACACS+ Authorization on page 93](#)

- TACACS+ authorization

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

- [Enabling TACACS+ Authentication on page 92](#)
- [Configuring TACACS+ Authorization on page 93](#)

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 419](#).
- [Configuring RADIUS Accounting on page 89](#)
- [Configuring TACACS+ Accounting on page 94](#)

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 and CPM 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

Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure security and provides the CLI commands. [Table 8](#) 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 8: Security Configuration Requirements

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

Security Configuration Procedures

- [Configuring Management Access Filters on page 72](#)
 - [Configuring IP CPM Filters Policy on page 75](#)
 - [Configuring MAC CPM Filters on page 76](#)
 - [Configuring CPM Queues on page 77](#)
 - [Configuring Profiles on page 80](#)
 - [Configuring Users on page 81](#)
 - [Copying and Overwriting Users and Profiles on page 83](#)
 - [Enabling SSH on page 95](#)
-

Configuring Management Access Filters

Creating and implementing management access filters is optional. Management access filters are software-based filters that 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 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 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 `keyword CPM` to be considered complete. Entries without the action keyword are considered incomplete and will be rendered inactive. Management Access Filter must have at least one active entry defined for the filter to be active.

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}
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

```

Configuring Management Access Filters

```
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 Policy

Use the following CLI commands to configure a CPM filter.

```
|ip-prefix-list prefix-list-name(10.0r4)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 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
    mac-filter
    shutdown
    entry 40 create
    action accept
    log 101
    match frame-type ethernet_II
    svc-id 12
    dst-mac 00:03:03:01:01 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. CPM filters and queues are not configurable on one-slot chassis.

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 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#
```

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 output 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 of a static lan-to-lan configuration using cert-auth:

interface "VPRN1" tunnel create

```
sap tunnel-1.private:1 create
  ipsec-tunnel "Sanity-1" create
    security-policy 1
    local-gateway-address 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
  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.

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. The following displays a user configuration example:

```
A:ALA-1>config>system>security# info
-----
...
    user "49ers"
        password "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
        access console ftp snmp
        restricted-to-home
        console
            member "default"
            member "ghost"
        exit
    exit
...
-----
A:ALA-1>config>system>security#
```

Configuring Keychains

The following displays a keychain configuration.

```
A:ALA-1>config>system>security# info
-----
...
        keychain "abc"
            direction
                bi
                    entry 1 key "ZcvSElJzJx/wBZ9biCtOVQJ9YZQvVU.S" hash2 alg
algorithm aes-128-cmac-96
                    begin-time 2006/12/18 22:55:20
                    exit
                exit
            exit
        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 user name 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 "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
        access snmp
        snmp
            authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
            group "testgroup"
        exit
    exit
    user "testuserA"
        password ""
        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 "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
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 ""
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"
```

Copying and Overwriting Users and Profiles

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

RADIUS Configurations

- [Configuring RADIUS Authentication on page 87](#)
- [Configuring RADIUS Authorization on page 88](#)
- [Configuring RADIUS Accounting on page 89](#)
- [Configuring 802.1x RADIUS Policies on page 90](#)

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 7450 ESS 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 87](#).

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\) on page 51](#).

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 7450 ESS 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]
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 7450 ESS-6/7/12 platforms. These features are not available on the 7450 ESS-1.

For more information about CPU protection, see “CPU Protection” and “Monitoring Attacks on the 7750 SR” sections in *SR OS Security Best Practices*.

TACACS+ Configurations

- [Enabling TACACS+ Authentication on page 92](#)
 - [Configuring TACACS+ Authorization on page 93](#)
 - [Configuring TACACS+ Accounting on page 94](#)
-

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 92](#).

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](#)
 - [LLDP Commands on page 98](#)
 - [Management Access Filter Commands on page 99](#)
 - [CLI Script Authorization Commands on page 100](#)
 - [CPM Filter Commands on page 100](#)
 - [CPM Queue Commands on page 102](#)
 - [CPU Protection Commands on page 103](#)
 - [Distributed CPU Protection Commands on page 104](#)
 - [Security Password Commands on page 105](#)
 - [Public Key Infrastructure \(PKI\) Commands on page 106](#)
 - [Profile Commands on page 106](#)
 - [RADIUS Commands on page 108](#)
 - [SSH Commands on page 108](#)
 - [TACPLUS Commands on page 108](#)
 - [User Commands on page 109](#)
 - [User Template Commands on page 109](#)
 - [Dot1x Commands on page 109](#)
 - [Keychain Commands on page 110](#)
 - [TTL Security Commands on page 110](#)
- [Login Control Commands on page 111](#)
- [Show Commands on page 112](#)
- [Clear Commands on page 113](#)
- [Debug Commands on page 113](#)
- [Tools Commands on page 113](#)

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 application6
      — [no] telnet-server
      —
```

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
```

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
— [no] log
— protocol protocol-id
— no protocol
— router {router-instance}
— no router
— src-ip {ip-prefix/mask | ip-prefix netmask}
— no src-ip
— src-port {port-id | cpm | lag lag-id }
— no src-port
— src-port 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..0xffff
— 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**

CLI Script Authorization Commands

- config
 - system
 - security
 - cli-script
 - authorization
 - cron
 - cli-user *user-name*
 - **[no] cli-user**
 - vsd
 - cli-user *user-name*
 - **[no] cli-user**
 - event-handler
 - cli-user *user-name*
 - **no cli-user**

CPM Filter Commands

- config
 - system
 - security
 - **[no] cpm-filter**
 - **default-action** {**accept** | **drop**}
 - **[no] ip-filter**
 - **[no] entry** *entry-id*
 - **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* | **ip-prefix-list** *prefix-list-name*}
 - **no dst-ip**
 - **dst-port** [**tcp/udp** *port-number*] [*mask*]
 - **no dst-port**
 - **fragment** {**true** | **false**}
 - **no fragment**
 - **icmp-code** *icmp-code*
 - **no icmp-code**
 - **icmp-type** *icmp-type*
 - **no icmp-type**
 - **ip-option** [*ip-option-value*] [*ip-option-mask*]
 - **no ip-option**
 - **multiple-option** {**true** | **false**}
 - **no multiple-option**
 - **option-present** {**true** | **false**}
 - **no option-present**
 - **port** *port-number*
 - **port -list** *port-list-name*

```

— port-range start end
— no port
— router
— 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

src-portsrc-port

— [no] mac-filter
— [no] entry entry-id
— description description-string
— no description
— log log-id
— no log
— 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..0xffff
— 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

```

Command Hierarchies

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
        — ip-src-monitoring
          — included-protocols
            — [no] dhcp
            — [no] gtp
            — [no] icmp
            — [no] igmp
        — 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 [log-events]
          — 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 [action-low-priority]
        — no port-overall-rate
        — [no] protocol-protection [allow-sham-links][block-pim-tunneled]

```

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 ]

```

Distributed CPU Protection Commands

```

config
  — system
    — security
      — dist-cpu-protection
        — policy policy-name [create]
        — no policy
          — description description-string
          — no description
          — [no] local-monitoring-policer policer-name [create]
            — [no] description "description-string"
            — rate {packets {ppi | max} within seconds [initial-delay packets] | kbps {kilobits-per-second | max} [mbs size] [bytes|kilobytes]}
            — no rate
            — [no] log-events [verbose]
        — protocol name [create]
        — no protocol name
          — dynamic-parameters
            — detection-time seconds
            — exceed-action {discard [hold-down seconds] | low-priority [hold-down seconds] | none}
            — log-events [verbose]
            — no log-events
            — rate {packets {ppi | max} within seconds [initial-delay packets] | kbps {kilobits-per-second | max} [mbs size] [bytes|kilobytes]}
            — enforcement {static policer-name | dynamic {mon-policer-name | local-mon-bypass }}
        — static-policer policer-name [create]
        — no static-policer policer-name
          — description description-string
          — no description
          — detection-time seconds
          — no detection-time
          — exceed-action {discard [hold-down seconds] | low-priority [hold-down seconds] | none}
          — log-events [verbose]
          — no log-events

```



```

— rate {packets {ppi | max} within seconds [initial-delay
      packets] | kbps {kilobits-per-second | max} [mbs size]
      [bytes|kilobytes]}
— no rate

config card x fp y
— dist-cpu-protection
— [no] dynamic-enforcement-policer-pool number-of-policers

```

Security Password Commands

```

config
— system
— security
— password
— admin-password password [hash | hash2]
— no admin-password
— aging days
— no aging
— attempts count [time minutes1] [lockout minutes2]
— no attempts
— authentication-order [method-1] [method-2] [method-3] [exit-on-reject]
— no authentication-order
— complexity-rules
— [no] allow-user-name
— credits [lowercase credits] [uppercase credits] [numeric credits]
  [special-character credits]
— no credits
— minimum-classes minimum
— no minimum-classes
— minimum-length length
— no minimum-length
— repeated-characters count
— no repeated-characters
— required [lowercase count] [uppercase count] [numeric count]
  [special-character count]
— no required
— dynsvc-password password [hash|hash2]
— no dynsvc-password
— enable-admin-control
— tacplus-map-to-priv-lvl admin-priv-lvl
— no tacplus-map-to-priv-lvl
— health-check [interval interval]
— no health-check
— history size
— no history
— minimum-age [days days] [hrs hours] [min minutes] [sec seconds]
— no minimum-age
— minimum-change distance
— no minimum-change

```

Public Key Infrastructure (PKI) Commands

```

config
  — system
    — security
      — pki
        — ca-profile name [create]
        — no ca-profile name
          — cert-file filename
          — no cert-file
          — [no] accept-unprotected-errormsg
          — [no] accept-unprotected-pkiconf
          — http-response-timeout timeout
          — no http-response-timeout
          — key-list
            — key password [hash|hash2] reference reference-number
            — no key reference reference-number
          — response-signing-cert filename
          — no response-signing-cert
          — [no] same-recipnonce-for-pollreq
          — url url-string [service-id service-id]
          — no url
        — certificate-display-format {ascii|utf8}
        — certificate-expiration-warning hours [repeat repeat-hours]
        — no certificate-expiration-warning
        — crl-expiration-warning hours [repeat repeat-hours]
        — no crl-expiration-warning
        — maximum-cert-chain-depth level
        — no maximum-cert-chain-depth

admin
  — certificate
    — clear-ocsp-cache [entry-id]
    — 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 [hash-alg hash-algorithm]
    — import type {cert|key|crl} input url-string output filename format input-format [password [32
      chars max]]
    — reload type {cert|key|cert-key-pair} filename [key-file 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
        — [no] interactive-authentication
        — 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
        — client-cipher-list protocol-version version
          — cipher index name cipher-name
          — no cipher index
        — [no] preserve-key
        — server-cipher-list protocol-version version
          — cipher index name cipher-name
          — no cipher index
        — [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 [use-priv-lvl]
        — [no] interactive-authentication
        — [no] priv-lvl-map
          — priv-lvl priv-lvl user-profile-name
          — no priv-lvl priv-lvl
        — 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]
 — [no] restricted-to-home
 — rsa-key public-key-value key-id
 — no rsa-key key-id
 — 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

```

## Command Hierarchies

- **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**
              - **option** {**basic** | **isis-enhanced**}
              - **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**
                - **option** {**basic** | **isis-enhanced**}
      - **[no] shutdown**
      - **tcp-option-number**
        - **receive** *option-number*
        - **send** *option-number*

## TTL Security Commands

- 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-filtermac-filter** [*entry entry-id*]
- **cpm-queue** *queue-id*
- **cpu-protection**
  - **eth-cfm-monitoring** [ {*service-id service-id sap-id sap-id*} | {*service-id service-id sdp-id sdp-id:vc-id*} ]
  - **excessive-sources** [*service-id service-id sap-id sap-id*]
  - **policy** [*policy-id*] **association**
  - **protocol-protection**
  - **violators** [*port*] [*interface*] [*sap*] [*video*] [*sdp*]
- **dist-cpu-protection**
  - **policy** [*policy-id*] [*association detail*]
- **keychain** *keychain-name* [*detail*]
- **management-access-filter**
  - **ip-filter** [*entry entry-id*]
  - **ipv6-filtermac-filter** [*entry entry-id*]
- **password-options**
- **per-peer-queuing** [*detail*]
- **per-peer-queuing**
- **profile** [*user-profile-name*]
- **source-address**
- **ssh**
- **user** [*user-name*] [*detail*]
- **user** [*user-name*] **lockout**
- **view** [*view-name*] [*detail*]

##### — certificate

- **ca-profile**
- **ca-profile** *name* [*association*]
- **ocsp-cache** [*entry-id*]
- **statistics**

#### show

##### — card

##### — fp

- **dist-cpu-protection**

#### show

##### — service

##### — id

##### — sap

- **dist-cpu-protection** [*detail*]



```

show
 — router
 — interface
 — dist-cpu-protection [detail]

```

## Login Control

```

show
 — user

```

## Clear Commands

```

clear
 — router
 — authentication
 — statistics [interface ip-int-name | ip-address]
 — radius-proxy-server server-name statistics
 — cpm-filter
 — ip-filter [entry entry-id]
 — ipv6-filtermac-filter [entry entry-id]
 — cpu-protection
 — excessive-sources
 — protocol-protection
 — violators [port] [interface] [sap]
 — cpm-queue queue-id
admin
 — user
 — user
 — clear lockout {name | all}
 — clear password-history {name | all}

```

## Debug Commands

```

debug
 — radius [detail] [hex]
 — no radius
 — [no] ocsp
 — [no] ocsp profile-name

```

## Tools Commands

```

tools
 — dump
 — security
 — dist-cpu-protection
 — violators enforcement {sap|interface} card slot-number [fp fp-number]
 — violators local-monitor {sap|interface} card slot-number [fp fp-number]
 — perform
 — security
 — dist-cpu-protection
 — release-hold-down interface interface-name [protocol protocol] [static-policer name]
 — release-hold-down sap sap-id [protocol protocol] [static-policer name]

```



---

## Configuration Commands

---

### General Security Commands

---

#### description

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>description</b> <i>description-string</i><br><b>no description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter>entry<br>config>sys>sec>cpm>ip-filter>entry<br>config>sys>sec>cpm>mac-filter>entry<br>config>sys>security>keychain>direction>bi>entry<br>config>system>security>keychain>direction>uni>receive>entry<br>config>system>security>keychain>direction>uni>send>entry<br>config>system>security>pki>ca-profile<br>config>sys>security>cpu-protection>policy<br>config>system>security>mgmt-access-filter>mac-filter>entry<br>config>system>security>cpm-filter>mac-filter>entry |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command removes the string.                                                                                                                                                                                                                                  |
| <b>Default</b>     | No description associated with the configuration context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <i>string</i> — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.                                                                                                                                                                                                                                              |

#### shutdown

|                |                                                                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>[no] shutdown</b>                                                                                                                                                                                     |
| <b>Context</b> | config>system>security>mgmt-access-filter>ip-filter<br>config>sys>sec>cpm>ip-filter<br>config>system>security>keychain>direction>bi>entry<br>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>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.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | all — read-version set to accept both versions 1 and 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b> | <p><b>read-version</b> {1   2   all} — When the read-version is configured as “all,” both versions 1 and 2 will be accepted by the system. Otherwise, only the selected version will be accepted when reading configuration or exec files. The presence of incorrect hash versions will abort the script/startup.</p> <p><b>write-version</b> {1   2} — Select the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.</p> |

## per-peer-queuing

|                    |                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] per-peer-queuing                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command disables CPM hardware queuing per peer.</p> |
| <b>Default</b>     | per-peer-queuing                                                                                                                                                                                                                                                                       |

## source-address

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | source-address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | <p>This command specifies the source address that should be used in all unsolicited packets sent by the application.</p> <p>This feature only applies on 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.</p> <p>When a source address is specified for the <b>ptp</b> application, the port-based 1588 hardware timestamping assist function will be applied to PTP packets matching the IPv4 address of the router interface used to ingress the SR/ESS or IP address specified in this command. If the IP address is removed, then the port-based 1588 hardware timestamping assist function will only be applied to PTP packets matching the IPv4 address of the router interface.</p> |

## application

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>application</b> <i>app</i> [ <i>ip-int-name</i>   <i>ip-address</i> ]<br><b>no application</b> <i>app</i>                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>system>security>source-address                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command specifies the use of the source IP address specified by the <b>source-address</b> command.                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>app</i> — Specify the application name.<br><br><b>Values</b> cflowd, dns, ftp, ntp, ping, ptp, radius, snmptrap, snmp, ssh, syslog, tacplus, telnet, traceroute, mcreporter<br><br><i>ip-int-name</i>   <i>ip-address</i> — 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

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

### telnet-server

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] telnet-server</b>                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command enables Telnet servers running on the system.</p> <p>Telnet servers are off by default. At system startup, only SSH servers are enabled.</p> <p>Telnet servers in networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries.</p> <p>The <b>no</b> form of the command disables Telnet servers running on the system.</p> |

---

## LLDP Commands

### lldp

|                    |                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>lldp</b>                                                                                         |
| <b>Context</b>     | config>system                                                                                       |
| <b>Description</b> | This command enables the context to configure system-wide Link Layer Discovery Protocol parameters. |

### message-fast-tx

|                    |                                                                                                                                                                               |               |          |                |   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------|----------------|---|
| <b>Syntax</b>      | <b>message-fast-tx</b> <i>time</i><br><b>no message-fast-tx</b>                                                                                                               |               |          |                |   |
| <b>Context</b>     | config>system>lldp                                                                                                                                                            |               |          |                |   |
| <b>Description</b> | This command configures the duration of the fast transmission period.                                                                                                         |               |          |                |   |
| <b>Parameters</b>  | <i>time</i> — Specifies the fast transmission period in seconds.<br><table><tr><td><b>Values</b></td><td>1 — 3600</td></tr><tr><td><b>Default</b></td><td>1</td></tr></table> | <b>Values</b> | 1 — 3600 | <b>Default</b> | 1 |
| <b>Values</b>      | 1 — 3600                                                                                                                                                                      |               |          |                |   |
| <b>Default</b>     | 1                                                                                                                                                                             |               |          |                |   |

### message-fast-tx-init

|                    |                                                                                                                                                                                                       |               |       |                |   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------|----------------|---|
| <b>Syntax</b>      | <b>message-fast-tx-init</b> <i>count</i><br><b>no message-fast-tx-init</b>                                                                                                                            |               |       |                |   |
| <b>Context</b>     | config>system>lldp                                                                                                                                                                                    |               |       |                |   |
| <b>Description</b> | This command configures the number of LLDPDUs to send during the fast transmission period.                                                                                                            |               |       |                |   |
| <b>Parameters</b>  | <i>count</i> — Specifies the number of LLDPDUs to send during the fast transmission period.<br><table><tr><td><b>Values</b></td><td>1 — 8</td></tr><tr><td><b>Default</b></td><td>4</td></tr></table> | <b>Values</b> | 1 — 8 | <b>Default</b> | 4 |
| <b>Values</b>      | 1 — 8                                                                                                                                                                                                 |               |       |                |   |
| <b>Default</b>     | 4                                                                                                                                                                                                     |               |       |                |   |

## notification-interval

|                    |                                                                                     |
|--------------------|-------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>notification-interval</b> <i>time</i><br><b>no notification-interval</b>         |
| <b>Context</b>     | config>system>lldp                                                                  |
| <b>Description</b> | This command configures the minimum time between change notifications.              |
| <b>Parameters</b>  | <i>time</i> — Specifies the minimum time, in seconds, between change notifications. |
| <b>Values</b>      | 5 — 3600                                                                            |
| <b>Default</b>     | 5                                                                                   |

## reinit-delay

|                    |                                                                                      |
|--------------------|--------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>reinit-delay</b> <i>time</i><br><b>no reinit-delay</b>                            |
| <b>Context</b>     | config>system>lldp                                                                   |
| <b>Description</b> | This command configures the time before re-initializing LLDP on a port.              |
| <b>Parameters</b>  | <i>time</i> — Specifies the time, in seconds, before re-initializing LLDP on a port. |
| <b>Values</b>      | 1 — 10                                                                               |
| <b>Default</b>     | 2                                                                                    |

## tx-credit-max

|                    |                                                                       |
|--------------------|-----------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tx-credit-max</b> <i>count</i><br><b>no tx-credit-max</b>          |
| <b>Context</b>     | config>system>lldp                                                    |
| <b>Description</b> | This command configures the maximum consecutive LLDPDUs transmitted.  |
| <b>Parameters</b>  | <i>count</i> — Specifies the maximum consecutive LLDPDUs transmitted. |
| <b>Values</b>      | 1 — 100                                                               |
| <b>Default</b>     | 5                                                                     |



## tx-hold-multiplier

|                    |                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tx-hold-multiplier</b> <i>multiplier</i><br><b>no tx-hold-multiplier</b>                                  |
| <b>Context</b>     | config>system>lldp                                                                                           |
| <b>Description</b> | This command configures the multiplier of the tx-interval.                                                   |
| <b>Parameters</b>  | <i>multiplier</i> — Specifies the multiplier of the tx-interval.<br><b>Values</b> 2 — 10<br><b>Default</b> 4 |

## tx-interval

|                    |                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tx-interval</b> <i>interval</i><br><b>no tx-interval</b>                                               |
| <b>Context</b>     | config>system>lldp                                                                                        |
| <b>Description</b> | This command configures the LLDP transmit interval time.                                                  |
| <b>Parameters</b>  | <i>interval</i> — Specifies the LLDP transmit interval time.<br><b>Values</b> 1 — 100<br><b>Default</b> 5 |

---

## Login, Telnet, SSH and FTP Commands

### exponential-backoff

|                    |                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] exponential-backoff</b>                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>system>login-control                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>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 <b>admin</b> with any conceivable password.</p> <p>The <b>no</b> form of the command disables exponential-backoff.</p> |
| <b>Default</b>     | no exponential-backoff                                                                                                                                                                                                                                                                                                                     |

### ftp

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

### idle-timeout

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

## inbound-max-sessions

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

## inbound-max-sessions

|                    |                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>inbound-max-sessions</b> <i>value</i><br><b>no inbound-max-sessions</b>                                                                                                                                                                                     |
| <b>Context</b>     | config>system>login-control>telnet                                                                                                                                                                                                                             |
| <b>Description</b> | 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.<br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | 5                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <i>value</i> — The maximum number of concurrent inbound Telnet sessions, expressed as an integer.<br><b>Values</b> 0 — 15                                                                                                                                      |

## login-banner

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

## login-control

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

## motd

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>motd</b> { <i>url url-prefix: source-url</i>   <b>text</b> <i>motd-text-string</i> }<br><b>no motd</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>system>login-control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command creates the message of the day displayed after a successful console login. Only one message can be configured.</p> <p>The <b>no</b> form of the command removes the message.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Default</b>     | No <b>motd</b> is defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <p><b>url</b> <i>url-prefix: source-url</i> — When the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote.</p> <p><b>text</b> <i>motd-text-string</i> — The text of the message of the day. The <i>motd-text-string</i> must be enclosed in double quotes. Multiple text strings are not appended to one another.</p> <p>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.</p> |

## outbound-max-sessions

|                    |                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>outbound-max-sessions</b> <i>value</i><br><b>no outbound-max-sessions</b>                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>login-control>telnet                                                                                                                                                                                                                                           |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command reverts to the default value.</p> |
| <b>Default</b>     | 5                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <p><i>value</i> — The maximum number of concurrent outbound Telnet sessions, expressed as an integer.</p> <p><b>Values</b>      0 — 15</p>                                                                                                                                   |

## pre-login-message

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

## ssh

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

## client-cipher-list protocol-version

|                    |                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>client-cipher-list protocol-version</b> <i>version</i>                                                                                                                                    |
| <b>Context</b>     | config>system>security>ssh                                                                                                                                                                   |
| <b>Description</b> | This command enables configuration the list of allowed ciphers by the SSH client.                                                                                                            |
| <b>Parameters</b>  | <p><i>version</i> — Specifies the SSH version.</p> <p><b>Values</b>      1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1</p> |

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

## cipher

**Syntax** **cipher** *index name cipher-name*  
**no cipher** *index*

**Context** config>system>security>ssh>client-cipher-list  
 config>system>security>ssh>server-cipher-list

**Description** This command enables configuration of a cipher. Client-ciphers are used when the SR OS is acting as an SSH client. Server-ciphers are used when the SR OS is acting as an SSH server.

**Parameters** *index* — Specifies the index of the cipher in the list.

**Values** 1 — 255

*cipher-name* — Specifies the algorithm for performing encryption or decryption.

**Values** For SSHv1:  
 Client ciphers: des, 3des, blowfish  
 Server ciphers: 3des, blowfish  
 The following default ciphers are used for SSHv1:

| Cipher index value | Cipher name |
|--------------------|-------------|
| 10                 | 3des        |
| 20                 | blowfish    |
| 30                 | des         |

**Values** For SSHv2:  
 Client ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr  
 Server ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr  
 The following default ciphers are used for SSHv2:

| Cipher index value | Cipher name  |
|--------------------|--------------|
| 190                | aes256-ctr   |
| 192                | aes192-ctr   |
| 194                | aes128-ctr   |
| 200                | aes128-cbc   |
| 205                | 3des-cbc     |
| 210                | blowfish-cbc |

|                | Cipher index value     | Cipher name  |
|----------------|------------------------|--------------|
|                | 215                    | cast128-cbc  |
|                | 220                    | arcfour      |
|                | 225                    | aes192-cbc   |
|                | 230                    | aes256-cbc   |
|                | 235                    | rijndael-cbc |
| <b>Default</b> | no cipher <i>index</i> |              |

## disable-graceful-shutdown

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

## preserve-key

|                    |                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] preserve-key</b>                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>system>security>ssh                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | 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.<br>The <b>no</b> 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. |
| <b>Default</b>     | no preserve-key                                                                                                                                                                                                                                                                                                                 |

## server-cipher-list protocol-version

|                    |                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>client-cipher-list protocol-version <i>version</i></b>                                                       |
| <b>Context</b>     | config>system>security>ssh                                                                                      |
| <b>Description</b> | This command enables configuration the list of allowed ciphers by the SSH server.                               |
| <b>Parameters</b>  | <i>version</i> — Specifies the SSH version.                                                                     |
| <b>Values</b>      | 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

### server-shutdown

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

### version

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |               |                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>version <i>ssh-version</i></b><br><b>no version</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |               |                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>system>security>ssh                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |               |                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | Specifies the SSH protocol version that will be supported by the SSH server.                                                                                                                                                                                                                                                                                                                                                                                                                            |               |                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default</b>     | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |               |                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <i>ssh-version</i> — Specifies the SSH version.<br><table><tr><td><b>Values</b></td><td>1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1<br/>2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2<br/>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.</td></tr></table> | <b>Values</b> | 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1<br>2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2<br>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. |
| <b>Values</b>      | 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1<br>2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2<br>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

|                    |                                                                                    |
|--------------------|------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>telnet</b>                                                                      |
| <b>Context</b>     | config>system>login-control                                                        |
| <b>Description</b> | This command creates the context to configure the Telnet login control parameters. |

### enable-graceful-shutdown

|               |                                      |
|---------------|--------------------------------------|
| <b>Syntax</b> | <b>[no] enable-graceful-shutdown</b> |
|---------------|--------------------------------------|



|                    |                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>login-control>telnet                                                                                                                 |
| <b>Description</b> | <p>This command enables graceful shutdown of telnet sessions.</p> <p>The no form of the command disables graceful shutdown of telnet sessions.</p> |

---

## Management Access Filter Commands

### management-access-filter

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

### ip-filter

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

### mac-filter

|                    |                                                         |
|--------------------|---------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] mac-filter</b>                                  |
| <b>Context</b>     | config>system>security>mgmt-access-filter               |
| <b>Description</b> | This command configures a management access MAC-filter. |

### action

|                    |                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>action {permit   deny   deny-host-unreachable}</b><br><b>no action</b>                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter>entry                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command creates the action associated with the management access filter match criteria entry.</p> <p>The <b>action</b> keyword is required. If no <b>action</b> is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.</p> |

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

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | none — The action is specified by default-action command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b> | <p><i>permit</i> — Specifies that packets matching the configured criteria will be permitted.</p> <p><b>deny</b> — Specifies that packets matching the configured selection criteria will be denied and that a ICMP host unreachable message will not be issued.</p> <p><b>deny-host-unreachable</b> — Specifies that packets matching the configured selection criteria will be denied and that a host unreachable message will not be issued.</p> <p><b>Note:</b> deny-host-unreachable only applies to ip-filter and ipv6filter.</p> |

## default-action

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-action {permit   deny   deny-host-unreachable}</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter<br>config>system>security>mgmt-access-filter>mac-filter                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | <p>This command creates the default action for management access in the absence of a specific management access filter match.</p> <p>The <b>default-action</b> 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 <b>default-action</b> must be defined.</p>                                                                                                                                                                                     |
| <b>Default</b>     | No default-action is defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <p><b>permit</b> — Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.</p> <p><b>deny</b> — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued.</p> <p><b>deny-host-unreachable</b> — Specifies that packets not matching the selection criteria be denied access and that an ICMP host unreachable message will be issued. <b>Note:</b> deny-host-unreachable only applies to ip-filter and ipv6filter.</p> |

## dst-port

|                    |                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] dst-port value [mask]</b>                                                                                                                                                                              |
| <b>Context</b>     | config>system>security>mgmt-access-filter>entry                                                                                                                                                                |
| <b>Description</b> | <p>This command configures a source TCP or UDP port number or port range for a management access filter match criterion.</p> <p>The <b>no</b> form of the command removes the source port match criterion.</p> |
| <b>Default</b>     | 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       | 0BBBBBBBBBBBBBBBB | 0b1111100000000000 |

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

**Default** 65535 (exact match)

**Values** 1 — 65535 (decimal)

## entry

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

**Context** config>system>security>mgmt-access-filter>ip-filter  
config>system>security>mgmt-access-filter>mac-filter

**Description** This command is used to create or edit a management access IP(v4), IPv6, or MAC filter entry. Multiple entries can be created with unique *entry-id* numbers. The 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

## log

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

|                    |                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter>entry<br>config>system>security>mgmt-access-filter>mac-filter                 |
| <b>Description</b> | This command enables match logging. When enabled, matches on this entry will cause the Security event mafEntryMatch to be raised. |
| <b>Default</b>     | no log                                                                                                                            |

## protocol

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

## port

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port</b> <i>tcp/udp</i> <i>port-number</i> [ <i>mask</i> ]<br><b>port-list</b> <i>port-list-name</i><br><b>port range</b> <i>start end</i><br><b>no port</b>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>system-security>cpm-filter>ip-filter>entry>match<br>config>system>security>cpm-filter>ipv6-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | <p>This command configures a TCP/UDP source or destination port match criterion in IPv4 and IPv6 CPM filter policies. A packet matches this criterion if packet's TCP/UDP (as configured by protocol/next-header match) source OR destination port matches either the specified port value or a port in the specified port range or port list.</p> <p>This command is mutually exclusive with <b>src-port</b> and <b>dst-port</b> commands.</p> <p>The <b>no</b> form of this command deletes the specified port match criterion.</p> |
| <b>Default</b>     | <b>no port</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>port-number</i> — A source or destination port to be used as a match criterion specified as a decimal integer.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Values</b>      | 1 -65535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

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

**Values** [0x0000..0xFFFF] | [0..65535] | [0b0000000000000000..0b1111111111111111]

**range** *start end* — an inclusive range of source or destination port values to be used as match criteria. *start* of the range and *end* of the range are expressed as decimal integers.

**Values** start, end, port-number: 1 -65535

**port-list** *port-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

### router

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>router</b> <i>service-name service-name</i><br><b>router</b> { <i>router-instance</i> }<br><b>no router</b>                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter>entry<br>config>system>security>mgmt-access-filter>ipv6-filter>entry                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | This command configures a router name or service ID to be used as a management access filter match criterion.<br><br>The <b>no</b> form the command removes the router name or service ID from the match criteria.                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>router-instance</i> — Specify one of the following parameters for the router instance:<br><br><i>router-name</i> — Specifies a router name up to 32 characters to be used in the match criteria.<br><i>service-id</i> — Specifies an existing service ID to be used in the match criteria.<br><br><b>Values</b> 1 — 2147483647<br><br><i>service-name service-name</i> — Specifies an existing service name up to 64 characters in length. |

### renum

|                    |                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>renum</b> <i>old-entry-number new-entry-number</i>                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter<br>config>system>security>mgmt-access-filter>mac-filter                                                                                                                                                                                                                                               |
| <b>Description</b> | This command renumbers existing management access filter entries for an IP(v4), IPv6, or MAC filter to re-sequence filter entries.<br><br>The exits on the first match found and executes the actions in accordance with the accompanying <b>action</b> command. This may require some entries to be re-numbered differently from most to least explicit. |
| <b>Parameters</b>  | <i>old-entry-number</i> — Enter the entry number of the existing entry.<br><br><b>Values</b> 1 — 9999                                                                                                                                                                                                                                                     |

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

**Values** 1 — 9999

## shutdown

|                    |                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                        |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter<br>config>system>security>mgmt-access-filter>mac-filter |
| <b>Description</b> | This command shutdowns the management-access-filter.                                                        |

## match

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

## cfm-opcode

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cfm-opcode {lt   gt   eq} opcode</b><br><b>cfm-opcode range start end</b><br><b>no cfm-opcode</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command specifies the type of opcode checking to be performed.</p> <p>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.</p> <p>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.</p> <p>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.</p> |

The following table provides opcode values.

**Table 9: Opcode Values**

| CFM PDU or Organization   | Acronym      | Configurable 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                                 |
|                           | IDM          | 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

**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

**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 |
| <b>Default</b> | FF (hex) (exact match) |            |
| <b>Values</b>  | 0x00 — 0xFF            |            |

### dst-mac

|                    |                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-mac</b> <i>ieee-address</i> [ <i>ieee-address-mask</i> ]<br><b>no dst-mac</b>                                                                                                                                                               |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                                                                                                                                                                                   |
| <b>Description</b> | This command configures the destination MAC match condition.                                                                                                                                                                                       |
| <b>Parameters</b>  | <i>ieee-address</i> — The MAC address to be used as a match criterion.<br><br><div> <b>Values</b> HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit </div> <i>mask</i> — A 48-bit mask to match a range of MAC address values. |

## etype

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>etype</b> <i>0x0600xx0xffff</i><br><b>no etype</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The <b>no</b> form of the command removes the previously entered etype field as the match criteria.</p> |
| <b>Default</b>     | no etype                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <p><i>ethernet-type</i> — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.</p> <p><b>Values</b>      0x0600 — 0xFFFF</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## snap-oui

|                    |                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>snap-oui</b> {zero   non-zero}                                                                                                                                                                                                   |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                                                                                                                                                                    |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command removes the criterion from the match criteria.</p> |
| <b>Default</b>     | no snap-oui                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <p><b>zero</b> — Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.</p> <p><b>non-zero</b> — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.</p>         |

## snap-pid

|                    |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>snap-pid</b> <i>snap-pid</i><br><b>no snap-pid</b>                                       |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                            |
| <b>Description</b> | 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

**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 | 0x0FFFFFF000000 |
| Binary       | 0bBBBBBB...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 0xFFFFF000000

**Default** 0xFFFFFFFFFFFF (exact match)

**Values** 0x0000000000000000 — 0xFFFFFFFFFFFF

## ssap

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ssap</b> <i>ssap-value</i> [ <i>ssap-mask</i> ]<br><b>no ssap</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.</p> <p>This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.</p> <p>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.</p> <p>The <b>no</b> form of the command removes the ssap match criterion.</p> |
| <b>Default</b>     | no ssap                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <p><i>ssap-value</i> — The 8-bit ssap match criteria value in hex.</p> <p><b>Values</b>      0x00 — 0xFF</p> <p><i>ssap-mask</i> — This is optional and may be used when specifying a range of ssap values to use as the match criteria.</p>                                                                                                                                                                                                                                                                                                                                             |

## svc-id

|                    |                                                                                                                                                                                                                                  |                    |                |                  |                       |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------|------------------|-----------------------|
| <b>Syntax</b>      | <b>svc-id</b> <i>service-id</i><br><b>no svc-id</b>                                                                                                                                                                              |                    |                |                  |                       |
| <b>Context</b>     | config>system>security>mgmt-access-filter>mac-filter>entry>match                                                                                                                                                                 |                    |                |                  |                       |
| <b>Description</b> | This command specifies an existing svc-id to use as a match condition.                                                                                                                                                           |                    |                |                  |                       |
| <b>Parameters</b>  | <p><i>service-id</i> — Specifies a service-id to match.</p> <p><b>Values</b></p> <table> <tr> <td><i>service-id:</i></td><td>1 — 2147483647</td></tr> <tr> <td><i>svc-name:</i></td><td>64 characters maximum</td></tr> </table> | <i>service-id:</i> | 1 — 2147483647 | <i>svc-name:</i> | 64 characters maximum |
| <i>service-id:</i> | 1 — 2147483647                                                                                                                                                                                                                   |                    |                |                  |                       |
| <i>svc-name:</i>   | 64 characters maximum                                                                                                                                                                                                            |                    |                |                  |                       |

## src-port

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-port</b> { <i>port-id</i>   <b>cpm</b>   <b>lag</b> <i>port-id</i> }<br><b>no src-port</b>                                               |
| <b>Context</b>     | config>system>security>mgmt-access-filter>ip-filter>entry<br>config>system>security>mgmt-access-filter>ipv6-filter>entry                        |
| <b>Description</b> | This command restricts ingress management traffic to either the CPMCCM Ethernet port or any other logical port (for example LAG) 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   | <i>slot/mda/port[.channel]</i>   |
| encap-val | 0 for null<br>0 — 4094 for dot1q |
| ccag-id   | <i>ccag-id.path-id[cc-type]</i>  |
|           | ccag keyword                     |
|           | id 1 — 8                         |
|           | path-id a, b                     |
|           | cc-type .sap-net, .net-sap       |
|           | cc-id 0 — 4094                   |
| lag-id    | <i>lag-id</i>                    |
|           | lag keyword                      |
|           | id 1 — 800                       |
| cpm       | keyword                          |

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

## src-ip

**Syntax** [**no**] **src-ip** {[*ip-prefix/mask*] | [*ip-prefix*] | **ip-prefix-list** *prefix-list-name*}

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

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

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.

**ip-prefix-list** — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

*ip-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

*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

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

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

### enable-admin

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>enable-admin</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | <global>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p><b>NOTE:</b> See the description for the <b>admin-password</b> on the previous page. If the <b>admin-password</b> is configured in the config&gt;system&gt;security&gt;password context, then any user can enter the special administrative mode by entering the <b>enable-admin</b> command.</p> <p><b>enable-admin</b> is in the default profile. By default, all users are given access to this command.</p> <p>Once the <b>enable-admin</b> command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.</p> <p>The minimum length of the password is determined by the <b>minimum-length</b> command. The complexity requirements for the password is determined by the <b>complexity</b> command.</p> <p>There are two ways to verify that a user is in the enable-admin mode:</p> <ul style="list-style-type: none"> <li>• show users — Administrator can know which users are in this mode.</li> <li>• Enter the enable-admin command again at the root prompt and an error message will be returned.</li> </ul> |

```
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

|                |                                      |
|----------------|--------------------------------------|
| <b>Syntax</b>  | <b>aging days</b><br><b>no aging</b> |
| <b>Context</b> | config>system>security>password      |



|                    |                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command reverts to the default value.</p> |
| <b>Default</b>     | No aging is enforced.                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <p><i>days</i> — The maximum number of days the password is valid.</p> <p><b>Values</b> 1 — 500</p>                                                                                                                                                                                           |

## attempts

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>attempts</b> <i>count</i> [<i>time minutes1</i> [<i>lockout minutes2</i>]</p> <p><b>no attempts</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.</p> <p>If the threshold is exceeded, the user is locked out for a specified time period.</p> <p>If multiple <b>attempts</b> commands are entered, each command overwrites the previously entered command.</p> <p>The <b>no attempts</b> command resets all values to default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Default</b>     | <p><b>count</b>: 3</p> <p><b>time minutes</b>: 5</p> <p><b>lockout minutes</b>: 10</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <p><i>count</i> — The number of unsuccessful login attempts allowed for the specified <b>time</b>. This is a mandatory value that must be explicitly entered.</p> <p><b>Values</b> 1 — 64</p> <p><i>time minutes</i> — The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.</p> <p><b>Values</b> 0 — 60</p> <p><i>lockout minutes</i> — The lockout period in minutes where the user is not allowed to login. Allowed values are decimal integers.</p> <p><b>Values</b> 0 — 1440   infinite</p> <p>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.</p> <p><b>Default</b> 10</p> <p><b>Values</b> 0 — 1440</p> <p><b>Values</b> infinite; user is locked out and must wait until manually unlocked before any further attempts.</p> |

## authentication-order

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

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

## complexity-rules

|                    |                                                                 |
|--------------------|-----------------------------------------------------------------|
| <b>Syntax</b>      | <b>complexity-rules</b>                                         |
| <b>Context</b>     | config>system>security>password                                 |
| <b>Description</b> | This defines a list of rules for configurable password options. |

## allow-user-name

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] allow-user-name</b>                                                                                                                       |
| <b>Context</b>     | config>system>security>password>complexity-rules                                                                                                  |
| <b>Description</b> | The user name is allowed to be used as part of the password.<br>The <b>no</b> form of the command does not allow user name to be used as password |

## credits

|                    |                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>credits [lowercase credits] [uppercase credits] [numeric credits] [special-character credits]</b><br><b>no credits</b>                              |
| <b>Context</b>     | config>system>security>password>complexity-rules                                                                                                       |
| <b>Description</b> | The maximum credits given for usage of the different character classes in the local passwords.<br>The <b>no</b> form of the command resets to default. |
| <b>Default</b>     | no credits                                                                                                                                             |
| <b>Parameters</b>  | <i>credits</i> — The number of credits that can be used for each characters class.<br><b>Values</b> 0-10                                               |

## minimum-classes

|               |                                                                    |
|---------------|--------------------------------------------------------------------|
| <b>Syntax</b> | <b>minimum-classes <i>minimum</i></b><br><b>no minimum-classes</b> |
|---------------|--------------------------------------------------------------------|

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>password>complexity-rules                                                                 |
| <b>Description</b> | Force the use of at least this many different character classes<br>The no form of the command resets to default. |
| <b>Default</b>     | no minimum-classes                                                                                               |
| <b>Parameters</b>  | <i>minnum</i> — The minimum number of classes to be configured.<br><b>Values</b> 2-4                             |

## minimum-length

|                    |                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>minimum-length</b> <i>length</i><br><b>no minimum-length</b>                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | 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.<br>If multiple minimum-length commands are entered each command overwrites the previous entered command.<br>The <b>no</b> form of the command reverts to default value. |
| <b>Default</b>     | <b>minimum-length</b> 6                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>value</i> — The minimum number of characters required for a password.<br><b>Values</b> 1 — 8                                                                                                                                                                                                                                                                 |

## repeated-characters

|                    |                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>repeated-characters</b> <i>count</i><br><b>no repeated-characters</b>                                                |
| <b>Context</b>     | config>system>security>password>complexity-rules                                                                        |
| <b>Description</b> | The number of times a characters can be repeated consecutively.<br>The <b>no</b> form of the command resets to default. |
| <b>Default</b>     | no repeated-characters                                                                                                  |
| <b>Parameters</b>  | <i>count</i> — The minimum count of consecutively repeated characters.<br><b>Values</b> 2-8                             |

## required

|                    |                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>required</b> [ <i>lowercase count</i> ] [ <i>uppercase count</i> ] [ <i>numeric count</i> ] [ <i>special-character count</i> ]<br><b>no required</b> |
| <b>Context</b>     | config>system>security>password>complexity-rules                                                                                                        |
| <b>Description</b> | Force the minimum number of different character classes required.<br>The <b>no</b> form of the command resets to default.                               |
| <b>Default</b>     | no required                                                                                                                                             |
| <b>Parameters</b>  | <i>count</i> — The minimum count of characters classes.<br><b>Values</b> 0-10                                                                           |

## dynsvc-password

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dynsvc-password</b> <i>password</i> [ <i>hash</i>   <i>hash2</i> ]<br><b>no dynsvc-password</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | Configure the password which enables the user to configure dynamic services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>     | no dynsvc-password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>password</i> — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.<br><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> 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<br><b>hash2</b> — Specifies the key is entered in a more complex encrypted form. If the <b>hash2</b> parameter is not used, the less encrypted <b>hash</b> form is assumed. |

## enable-admin-control

|                    |                                                   |
|--------------------|---------------------------------------------------|
| <b>Syntax</b>      | <b>enable-admin-control</b>                       |
| <b>Context</b>     | config>system>security>password                   |
| <b>Description</b> | Enable the user to become a system administrator. |

## tacplus-map-to-priv-lvl

|               |                                                          |
|---------------|----------------------------------------------------------|
| <b>Syntax</b> | <b>tacplus-map-to-priv-lvl</b> [ <i>admin-priv-lvl</i> ] |
|---------------|----------------------------------------------------------|

### **no tacplus-map-to-priv-lvl**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>password>enable-admin-control                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | When <b>tacplus-map-to-priv-lvl</b> is enabled, and tacplus authorization is enabled with the <i>use-priv-lvl</i> option, typing <b>enable-admin</b> starts an interactive authentication exchange from the SR OS node to the TACACS+ server. The start message (service=enable) contains the user-id and the requested admin-priv-lvl. Successful authentication results in the use of a new profile (as configured under <b>config&gt;system&gt;security&gt;tacplus&gt;priv-lvl-map</b> ). |

## health-check

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] health-check [interval <i>interval</i>]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> 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.</p> |
| <b>Default</b>     | health-check 30                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <b>interval <i>interval</i></b> — Specifies the polling interval for RADIUS servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                    | <b>Values</b> 6 — 1500                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## history

|                    |                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>history <i>size</i></b><br><b>no history</b>                                               |
| <b>Context</b>     | config>system>security>password                                                               |
| <b>Description</b> | Configure how many previous passwords a new password is matched against.                      |
| <b>Default</b>     | no history                                                                                    |
| <b>Parameters</b>  | <b><i>size</i></b> — Specifies how many previous passwords a new password is matched against. |
|                    | <b>Values</b> 1—20                                                                            |

## minimum-age

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>minimum-age</b> [ <i>days days</i> ] [ <i>hrs hours</i> ] [ <i>min minutes</i> ] [ <b>sec seconds</b> ]<br><b>no minimum-age</b>                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | Configure the minimum required age of a password before it can be changed again.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>     | no minimum-age                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><i>days</i> — Specifies the minimum required days of a password before it can be changed again.</p> <p><b>Values</b> 0—1</p> <p><i>hours</i> — Specifies the minimum required hours of a password before it can be changed again.</p> <p><b>Values</b> 0—23</p> <p><i>minutes</i> — Specifies the minimum required minutes of a password before it can be changed again.</p> <p><b>Values</b> 0—59</p> <p><i>seconds</i> — Specifies the minimum required seconds of a password before it can be changed again.</p> <p><b>Values</b> 0—59</p> |

## minimum-change

|                    |                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>minimum-change</b> <i>length</i><br><b>no minimum-change</b>                                                                                                                                           |
| <b>Context</b>     | config>system>security>password                                                                                                                                                                           |
| <b>Description</b> | <p>This command configures the minimum number of characters required to be different in the new password from a previous password.</p> <p>The <b>no</b> form of the command reverts to default value.</p> |
| <b>Default</b>     | no min-change                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><i>length</i> — Specifies how many characters must be different in the new password from the old password.</p> <p><b>Values</b> 2—20</p>                                                               |

## password

|                    |                                                                               |
|--------------------|-------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>password</b>                                                               |
| <b>Context</b>     | config>system>security                                                        |
| <b>Description</b> | This command creates the context to configure password management parameters. |

---

## Public Key Infrastructure (PKI) Commands

### pki

|                    |                                                                       |
|--------------------|-----------------------------------------------------------------------|
| <b>Syntax</b>      | <b>pki</b>                                                            |
| <b>Context</b>     | config>system>security                                                |
| <b>Description</b> | This command enables the context to configure certificate parameters. |
| <b>Default</b>     | none                                                                  |

### ca-profile

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ca-profile</b> <i>name</i> [ <b>create</b> ]<br><b>no ca-profile</b> <i>name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>system>security>pki                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command creates a new <b>ca-profile</b> or enter the configuration context of an existing <b>ca-profile</b>. Up to 128 ca-profiles could be created in the system. A <b>shutdown</b> the ca-profile will not affect the current up and running <b>ipsec-tunnel</b> or <b>ipsec-gw</b> that associated with the <b>ca-profile</b>. But authentication afterwards will fail with a <b>shutdown ca-profile</b>.</p> <p>Executing a <b>no shutdown</b> command in this context will cause system to reload the configured cert-file and crl-file.</p> <p>A <b>ca-profile</b> can be applied under the <b>ipsec-tunnel</b> or <b>ipsec-gw</b> configuration.</p> <p>The <b>no</b> 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.</p> |
| <b>Parameters</b>  | <p><i>name</i> — Specifies the name of the <b>ca-profile</b>, a string up to 32 characters.</p> <p><b>create</b> — Keyword used to create a new <b>ca-profile</b>. The <b>create</b> keyword requirement can be enabled/disabled in the <b>environment&gt;create</b> context.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### cert-file

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cert-file</b> <i>filename</i><br><b>no cert-file</b>                                                                  |
| <b>Context</b>     | config>system>security>pki>ca-profile                                                                                    |
| <b>Description</b> | <p>Specifies the filename of a file in cf3:\system-pki\cert as the CA's certificate of the ca-profile.</p> <p>Notes:</p> |



- 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 RFC 5280 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 fail.

- 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.

## accept-unprotected-errormsg

|                    |                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] accept-unprotected-errormsg</b>                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>system>security>pki>ca-profile>cmpv2                                                                                                                                                                                                                                     |
| <b>Description</b> | This command enables the system to accept both protected and unprotected CMPv2 error message. Without this command, system will only accept protected error messages.<br>The <b>no</b> form of the command causes the system to only accept protected PKI confirmation message. |
| <b>Default</b>     | no                                                                                                                                                                                                                                                                              |

## accept-unprotected-pkiconf

|                    |                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] accept-unprotected-pkiconf</b>                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>pki>ca-profile>cmpv2                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command enables the system to accept both protected and unprotected CMPv2 PKI confirmation messages. Without this command, system will only accept protected PKI confirmation message.<br>The <b>no</b> form of the command causes the system to only accept protected PKI confirmation message. |

**Default** none

### key-list

**Syntax** **cmp-key-list**

**Context** config>system>security>pki>ca-profile>cmp2

**Description** This command enables the context to configure pre-shared key list parameters.

### key

**Syntax** **key password [hash|hash2] reference reference-number**  
**no key reference reference-number**

**Context** config>system>security>pki>ca-profile>cmp2>key-list

**Description** This command specifies a pre-shared key used for CMPv2 initial registration. Multiples of key commands are allowed to be configured under this context.

The password and reference-number is distributed by the CA via out-of-band means.

The configured password is stored in configuration file in an encrypted form by using SR OS hash2 algorithm.

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

**Default** none

**Parameters** *password* — Specifies a printable ASCII string, up to 64 characters in length.

**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.

**reference reference-number** — Specifies a printable ASCII string, up to 64 characters in length.

### url

**Syntax** **cmp-url url-string [service-id service-id]**  
**no cmp-url**

**Context** config>system>security>pki>ca-profile>cmp2

**Description** This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles.

The URL will be resolved by the DNS server configured (if configured) in the corresponding router context.

If the *service-id* is 0 or omitted, then system will try to resolve the FQDN via DNS server configured in *bof.cfg*. After resolution, the system will connect to the address in management routing instance first, then base routing instance.

Note that if the service is VPRN, then the system only allows HTTP ports 80 and 8080.

|                   |                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | none                                                                                                                                                                                                               |
| <b>Parameters</b> | <p><i>url-string</i> — Specifies the HTTP URL of the CMPv2 server up to 180 characters in length.</p> <p><b>service-id</b> <i>service-id</i> — Specifies the service instance that used to reach CMPv2 server.</p> |
| <b>Values</b>     | <p>service-id: 1..2147483647</p> <p>base-router: 0</p>                                                                                                                                                             |

## http-response-timeout

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-response-timeout</b> <i>timeout</i><br><b>no http-response-timeout</b>                                                                            |
| <b>Context</b>     | config>system>security>pki>ca-profile>cmp2                                                                                                                |
| <b>Description</b> | <p>This command specifies the timeout value for HTTP response that is used by CMPv2.</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| <b>Default</b>     | 30 seconds                                                                                                                                                |
| <b>Parameters</b>  | <p><i>timeout</i> — Specifies the HTTP response timeout in seconds.</p> <p><b>Values</b> 1 — 3600</p>                                                     |

## response-signing-cert

|                    |                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>response-signing-cert</b> <i>filename</i><br><b>no response-signing-cert</b>                                                                                                                                 |
| <b>Context</b>     | config>system>security>pki>ca-profile>cmp2                                                                                                                                                                      |
| <b>Description</b> | <p>This command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                            |
| <b>Parameters</b>  | <p><i>filename</i> — Specifies the filename of the imported certificate.</p>                                                                                                                                    |

## same-recipnonce-for-pollreq

|                    |                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] same-recipnonce-for-pollreq</b>                                                             |
| <b>Context</b>     | config>system>security>pki>ca-profile>cmp2                                                          |
| <b>Description</b> | This command enables the system to use same recipNonce as the last CMPv2 response for poll request. |
| <b>Default</b>     | none                                                                                                |

## crl-file

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>crl-file <i>filename</i></b><br><b>no crl-file</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>security>pki>ca-profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command specifies the name of a file in cf3:\system-pki\crl as the Certification Revoke List file of the <b>ca-profile</b>.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>The system will perform following checks against configured crl-file when a <b>no shutdown</b> command is issued: <ul style="list-style-type: none"> <li>→ A valid cert-file of the ca-profile must be already configured.</li> <li>→ Configured crl-file must be a DER formatted CRLv2 file.</li> <li>→ All non-optional fields defined in section 5.1 of RFC5280 must exist and conform to the RFC5280 defined format.</li> <li>→ Check the version field to see if its value is 0x1.</li> <li>→ Delta CRL Indicator must NOT exists (delta CRL is not supported).</li> <li>→ CRL's signature must be verified by using the cert-file of ca-profile.</li> </ul> <p>If any of above checks fail, the <b>no shutdown</b> command will fail.</p> </li> <li>Changing or removing the <b>crl-file</b> is only allowed when the <b>ca-profile</b> is in a <b>shutdown</b> state.</li> </ul> <p>The <b>no</b> form of the command removes the filename from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <i>filename</i> — Specifies the name of CRL file stored in cf3:\system-pki\crl.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## ocsp

|                    |                                                                |
|--------------------|----------------------------------------------------------------|
| <b>Syntax</b>      | <b>ocsp</b>                                                    |
| <b>Context</b>     | config>system>security>pki>ca-profile                          |
| <b>Description</b> | This command enables the context to configure OCSP parameters. |

## responder-url

|                    |                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>responder-url</b> <i>url-string</i><br><b>no responder-url</b>                                                                                                                          |
| <b>Context</b>     | config>system>security>pki>ca-profile>ocsp                                                                                                                                                 |
| <b>Description</b> | This command specifies HTTP URL of the OCSP responder for the CA, this URL will only be used if there is no OCSP responder defined in the AIA extension of the certificate to be verified. |
| <b>Default</b>     | no responder-url                                                                                                                                                                           |
| <b>Parameters</b>  | <i>url-string</i> — Specifies the HTTP URL of the OCSP responder                                                                                                                           |

## service

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>service</b> <i>service-id</i><br><b>no service</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>system>security>pki>ca-profile>ocsp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>This command specifies the service or routing instance that used to contact OCSP responder. This applies to OCSP responders that either configured in CLI or defined in AIA extension of the certificate to be verified.</p> <p>The responder-url will also be resolved by using the DNS server configured in the configured routing instance.</p> <p>In case of VPRN service, system will check if the specified service-id or service-name is an existing VPRN service at the time of CLI configuration. Otherwise the configuration will fail.</p> |
| <b>Parameters</b>  | <i>service-id</i> — Specifies an existing service ID to be used in the match criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Values</b>      | service-id: 1 — 2147483647<br>base-router: 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## certificate-display-format

|                    |                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>certificate-display-format</b> {ascii utf8}                                                                                                                                                                   |
| <b>Context</b>     | config>system>security>pki                                                                                                                                                                                       |
| <b>Description</b> | This command specifies the display format used for the Certificates and Certificate Revocation Lists.                                                                                                            |
| <b>Default</b>     | ascii                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>ascii</b> — Specifies the ASCII format to use for the Certificates and Certificate Revocation Lists.<br><b>utf8</b> — Specifies the UTF8 format to use for the Certificates and Certificate Revocation Lists. |

## certificate-expiration-warning

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>certificate-expiration-warning</b> <i>hours</i> [ <b>repeat</b> <i>repeat-hours</i> ]<br><b>no certificate-expiration-warning</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>system>security>pki                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | <p>With this command configured, the system will issues two types of warnings related to certificate expiration:</p> <ul style="list-style-type: none"> <li>• <b>BeforeExp</b> — A warning message issued before certificate expire</li> <li>• <b>AfterExp</b> — A warning message issued when certificate expire</li> </ul> <p>This command specifies when system will issue <b>BeforeExp</b> message before a certificate expires. For example, with <b>certificate-expiration-warning 5</b>, the system will issue a <b>BeforeExp</b> message 5 hours before a certificate expires. An optional <b>repeat</b> <i>&lt;repeat-hour&gt;</i> parameter will enable the system to repeat the <b>BeforeExp</b> message every hour until the certificate expires.</p> <p>If the user only wants <b>AfterExp</b>, then <b>certificate-expiration-warning 0</b> can be used to achieve this.</p> <p><b>BeforeExp</b> and <b>AfterExp</b> warnings can be cleared in following cases:</p> <ul style="list-style-type: none"> <li>• The certificate is reloaded by the <b>admin certificate reload</b> command. In this case, if the reloaded file is not expired, then <b>AfterExp</b> is cleared. And, if the reloaded file is outside of configured warning window, then the <b>BeforeExp</b> is also cleared.</li> <li>• When the <b>ca-profile/ipsec-gw/ipsec-tunnel/cert-profile</b> is shutdown, then <b>BeforeExp</b> and <b>AfterExp</b> of corresponding certificates are cleared.</li> <li>• When <b>no certificate-expiration-warning</b> command is configured, then all existing <b>BeforeExp</b> and <b>AfterExp</b> are cleared.</li> <li>• Users may change the configuration of the <b>certificate-expiration-warning</b> so that certain certificates are no longer in the warning window. <b>BeforeExp</b> of corresponding certificates are cleared.</li> <li>• If the system time changes so that the new time causes the certificates to no longer be in the warning window, then <b>BeforeExp</b> is cleared. If the new time causes an expired certificate to come non-expired, then <b>AfterExp</b> is cleared.</li> </ul> |
| <b>Default</b>     | no certificate-expiration-warning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                   |                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>hours</i> — Specifies the amount of time before a certificate expires when system issues <b>BeforeExp</b> . |
| <b>Values</b>     | 0 — 8760                                                                                                       |
|                   | <i>repeat repeat-hours</i> — The system will repeat <b>BeforeExp</b> every repeat-hour.                        |
| <b>Values</b>     | 0 — 8760                                                                                                       |

## crl-expiration-warning

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>crl-expiration-warning</b> <i>hours</i> [ <b>repeat</b> <i>repeat-hours</i> ]<br><b>no crl-expiration-warning</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>security>pki                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command specifies when system will issue <b>BeforeExp</b> message before a CRL expires. For example, with <b>certificate-expiration-warning 5</b>, the system will issue a <b>BeforeExp</b> message 5 hours before a CRL expires. An optional <b>repeat</b> &lt;<i>repeat-hour</i>&gt; parameter will enable the system to repeat the <b>BeforeExp</b> message every hour until the CRL expires.</p> <p>If the user only wants <b>AfterExp</b>, then <b>certificate-expiration-warning 0</b> can be used to achieve this.</p> <p><b>BeforeExp</b> and <b>AfterExp</b> warnings can be cleared in following cases:</p> <ul style="list-style-type: none"> <li>• The CRL is reloaded by the <b>admin certificate reload</b> command. In this case, if the reloaded file is not expired, then <b>AfterExp</b> is cleared. And, if the reloaded file is outside of configured warning window, then the <b>BeforeExp</b> is also cleared.</li> <li>• When the <b>ca-profile</b> is shutdown, then <b>BeforeExp</b> and <b>AfterExp</b> of corresponding certificates are cleared.</li> <li>• When <b>no crl-expiration-warning</b> command is configured, then all existing <b>BeforeExp</b> and <b>AfterExp</b> are cleared.</li> <li>• Users may change the configuration of the <b>crl-expiration-warning</b> so that certain CRL are no longer in the warning window. <b>BeforeExp</b> of corresponding CRL are cleared.</li> <li>• If the system time changes so that the new time causes the CRL to no longer be in the warning window, then <b>BeforeExp</b> is cleared. If the new time causes an expired CRL to come non-expired, then <b>AfterExp</b> is cleared.</li> </ul> |
| <b>Default</b>     | no crl-expiration-warning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <p><i>hours</i> — Specifies the amount of time before a CRL expires when system issues <b>BeforeExp</b>.</p> <p><b>Values</b> 0 — 8760</p> <p><i>repeat-hour</i> — Specifies that the system will repeat <b>BeforeExp</b> every repeat-hour.</p> <p><b>Values</b> 0 — 8760</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## maximum-cert-chain-depth

|               |                                              |
|---------------|----------------------------------------------|
| <b>Syntax</b> | <b>maximum-cert-chain-depth</b> <i>level</i> |
|---------------|----------------------------------------------|

### **no maximum-cert-chain-depth**

|                    |                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>pki                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | <p>This command defines the maximum depth of certificate chain verification. This number is applied system wide.</p> <p>The <b>no</b> form of the command reverts to the default.</p>                                                                                                                                               |
| <b>Default</b>     | 7                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><i>level</i> — 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.</p> <p><b>Values</b>      1 — 7</p> |

## shutdown

|                    |                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>pki>ca-profile>                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>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 <b>no shutdown</b> command will fail.</p> <p>The ca-profile in a <b>shutdown</b> state cannot be used in certificate authentication.</p> |
| <b>Default</b>     | shutdown                                                                                                                                                                                                                                                                                            |

## certificate

|                    |                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>certificate</b>                                                                              |
| <b>Context</b>     | admin                                                                                           |
| <b>Description</b> | This command enables the context to configure X.509 certificate related operational parameters. |

## clear-ocsp-cache

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>clear-ocsp-cache</b> [ <i>entry-id</i> ]                                                                                                               |
| <b>Context</b>     | admin>certificate                                                                                                                                         |
| <b>Description</b> | This command clears the current OCSP response cache. If optional issuer and serial-number are not specified, then all current cached results are cleared. |
| <b>Parameters</b>  | <p><i>entry-id</i> — Specifies the local cache entry identifier of the certificate to clear.</p> <p><b>Values</b>      1 — 2000</p>                       |



## 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:

**DefaultCertificate**

- system format
- PKCS #12
- PKCS #7 PEM encoded
- PKCS #7 DER encoded
- RFC4945
- Certificate Request
  - PKCS #10
- Key
  - system format
  - PKCS #12
- CRL
  - 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.

|               |            |                              |
|---------------|------------|------------------------------|
| <b>Values</b> | 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

|                    |                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>export type</b> {cert key crl} <b>input</b> <i>filename</i> <b>output</b> <i>url-string</i> <b>format</b> <i>output-format</i> [ <b>password</b> [32 chars max]] [ <b>pkey</b> <i>filename</i> ] |
| <b>Context</b>     | admin>certificate                                                                                                                                                                                   |
| <b>Description</b> | This command performs certificate operations.                                                                                                                                                       |

## gen-keypair

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                              |  |               |            |                              |  |           |                           |  |             |                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|--|---------------|------------|------------------------------|--|-----------|---------------------------|--|-------------|----------------|
| <b>Syntax</b>      | <b>gen-keypair</b> <i>url-string</i> [ <b>size</b> {512 1024 2048}] [ <b>type</b> {rsa dsa}]                                                                                                                                                                                                                                                                                                                                                                                                                                 |                              |  |               |            |                              |  |           |                           |  |             |                |
| <b>Context</b>     | admin>certificate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                              |  |               |            |                              |  |           |                           |  |             |                |
| <b>Description</b> | This command generatse a RSA or DSA private key/public key pairs and store them in a local file in cf3:\system-pki\key                                                                                                                                                                                                                                                                                                                                                                                                       |                              |  |               |            |                              |  |           |                           |  |             |                |
| <b>Parameters</b>  | <i>url-string</i> — Specifies the name of the key file. <table><tr><td><b>Values</b></td><td>url-string</td><td>&lt;local-url&gt; - [99 chars max]</td></tr><tr><td></td><td>local-url</td><td>&lt;cf-flash-id&gt;/&lt;file-path&gt;</td></tr><tr><td></td><td>cf-flash-id</td><td>cf1: cf2: cf3:</td></tr></table><br><b>size</b> — Specifies the key size in bits.<br>possible choice are 512/1024/2048; the default value is<br><b>Default</b> 2048<br><br><b>type</b> — Specifies the type of key.<br><b>Default</b> rsa |                              |  | <b>Values</b> | url-string | <local-url> - [99 chars max] |  | local-url | <cf-flash-id>/<file-path> |  | cf-flash-id | cf1: cf2: cf3: |
| <b>Values</b>      | url-string                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <local-url> - [99 chars max] |  |               |            |                              |  |           |                           |  |             |                |
|                    | local-url                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <cf-flash-id>/<file-path>    |  |               |            |                              |  |           |                           |  |             |                |
|                    | cf-flash-id                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | cf1: cf2: cf3:               |  |               |            |                              |  |           |                           |  |             |                |

## gen-local-cert-req

|                    |                                                                                                                                                                                                                                                   |             |                              |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------|
| <b>Syntax</b>      | <b>gen-local-cert-req</b> <b>keypair</b> <i>url-string</i> <b>subject-dn</b> <i>subject-dn</i> [ <b>domain-name</b> [255 chars max]] [ <b>ip-addr</b> <i>ip-address</i> ] <b>file</b> <i>url-string</i> [ <b>hash-alg</b> <i>hash-algorithm</i> ] |             |                              |
| <b>Context</b>     | admin>certificate                                                                                                                                                                                                                                 |             |                              |
| <b>Description</b> | This command generates a PKCS#10 formatted certificate request by using a local existing key pair file.                                                                                                                                           |             |                              |
| <b>Default</b>     | none                                                                                                                                                                                                                                              |             |                              |
| <b>Parameters</b>  | <i>url-string</i> — Specifies the name of the keyfile in cf3:\system-pki\key that is used to generate a certificate request.                                                                                                                      |             |                              |
|                    | <b>Values</b>                                                                                                                                                                                                                                     | url-string  | <local-url> - [99 chars max] |
|                    |                                                                                                                                                                                                                                                   | local-url   | <cf-flash-id>/<file-path>    |
|                    |                                                                                                                                                                                                                                                   | cf-flash-id | cf1: cf2: cf3:               |
|                    | <b>subject-dn</b> — Specifies the distinguish name that is used as the subject in a 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 including any of the 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=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 the dNSName in the Subject Alternative Name extension of the certificate request.

*ip-address* — Optionally, an IPv4 address string can be specified and included as the ipAddress in the 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 an FTP URL to upload the certificate request.

**hash-alg** *hash-algorithm* — Specifies the hash algorithm to be used in a certificate request.

**Values** sha1, sha224, sha256, sha384, sha512

## import

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>import type {cert key crl} input url-string output filename format input-format [password [32 chars max]]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | admin>certificate#                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command converts an input file(key/certificate/CRL) to a system format file. The following list summarizes the formats supported by this command:</p> <ul style="list-style-type: none"> <li>• Certificate <ul style="list-style-type: none"> <li>→ PKCS #12</li> <li>→ PKCS #7 PEM encoded</li> <li>→ PKCS #7 DER encoded</li> <li>→ PEM</li> <li>→ DER</li> </ul> </li> <li>• Key <ul style="list-style-type: none"> <li>→ PKCS #12</li> <li>→ PEM</li> <li>→ DER</li> </ul> </li> <li>• CRL <ul style="list-style-type: none"> <li>→ PKCS #7 PEM encoded</li> </ul> </li> </ul> |

- 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

|               |                   |                              |
|---------------|-------------------|------------------------------|
| <b>Values</b> | <i>url-string</i> | <local-url> - [99 chars max] |
|               | <i>local-url</i>  | <cflash-id>/<file-path>      |
|               | <i>cflash-id</i>  | 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**|**cert-key-pair**} *filename* [**key-file** *filename*]

**Context** admin>certificate

**Description** This command reloads imported certificate or key file or both at the same time. This command is typically used to update certificate/key file without shutting down **ipsec-tunne/ipsec-gw/cert-profile/ca-profile**. Note that **type cert** and **type key** will be deprecated in a future release. Use **type cert-key-pair** instead. Instead of **type cert** use **type key** instead.

- If the new file exists and valid, then for each tunnel using it:
  - If the key matches the certificate, then the new file will be downloaded to the MS-ISA to be used the next time. Tunnels currently up are not affected.
  - If the key does not match the certificate:
    - If **cert** and **key** configuration is used instead of **cert-profile** then the tunnel will be brought down.

- If **cert-profile** is used, then **cert-profile** will be brought down. The next authentication will fail while the established tunnels are not affected.

If the new file does not exist or is somehow invalid (bad format, does not contain right extension, etc.), then this command will abort.

In the case of **type cert-key-pair**, if the new file doesn't exist or is invalid or **cert** and **key** do not match, then this command will abort with an error message.

**Default** none

**Parameters**

- cert** — Specifies to reload a certificate file.
- key** — Specifies to reload a key file.
- cert-key-pair** — Specifies to reload a certificate file and its key file at the same time.
- file-name* — Specifies the file name of imported certificate or key.
- key-filename* — In case of cert-key-pair, filename is the imported filename of certificate, key-filename is the imported key file.

---

## Profile Management Commands

### action

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

### match

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>match <i>command-string</i></b><br><b>no match</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command configures a command or subtree commands in subordinate command levels are specified.</p> <p>Because the OS 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.</p> <p>All commands below the hierarchy level of the matched command are denied.</p> <p>The <b>no</b> form of this command removes a match condition</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b>  | <i>command-string</i> — The CLI command or CLI tree level that is the scope of the profile entry.                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### copy

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

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

## description

|                    |                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>description <i>description-string</i></b><br><b>no description</b>                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>This command creates a text description stored in the configuration file for a configuration context.</p> <p>The <b>description</b> command associates a text string with a configuration context to help identify the context in the configuration file.</p> <p>The <b>no</b> form of the command removes the string from the context.</p> |
| <b>Default</b>     | No description is configured.                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <i>string</i> — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.                                                              |

### entry

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

### profile

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

### renum

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



- Description** This command renumbers profile entries to re-sequence the entries.
- Since the OS 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

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

### authentication

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>authentication {[none]   [[hash] {md5 key-1   sha key-1} privacy {none des-key aes-128-cfb-key key-2}]}</b>                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>system>security>user>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command configures the authentication and encryption method the user must use in order to be validated by the router. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered.</p> <p>The keys configured in this command must be localized keys (MD5 or DES hash of the configured SNMP engine-ID and a password). The password is not directly entered in this command (only the localized key).</p> |
| <b>Default</b>     | <b>authentication none</b> - No authentication is configured and privacy cannot be configured.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <b>none</b> — Do not use authentication. If <b>none</b> 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-rules** 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-rules** 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

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

## cannot-change-password

**Syntax**      [no] **cannot-change-password**

|                    |                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>user>console                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | <p>This command allows a user the privilege to change their password for both FTP and console login.</p> <p>To disable a user's privilege to change their password, use the <b>cannot-change-password</b> form of the command.</p> <p>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.</p> |
| <b>Default</b>     | no cannot-change-password                                                                                                                                                                                                                                                                                                                                                             |

### console

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

### copy

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

### home-directory

|                    |                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>home-directory</b> <i>url-prefix</i> [ <i>directory</i> ] [ <i>directory/directory...</i> ]<br><b>no home-directory</b>         |
| <b>Context</b>     | config>system>security>user<br>config>system>security>user-template                                                                |
| <b>Description</b> | This command configures the local home directory for the user for both console (file commands and '>' redirection) 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*

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

### new-password-at-login

|                    |                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] new-password-at-login                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>user>console                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command does not force the user to change passwords.</p> |
| <b>Default</b>     | no new-password-at-login                                                                                                                                                                                                                                                            |

### password

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>password</b> [ <i>password</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>user                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command configures the user password for console and FTP access.</p> <p>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.</p> <p>The password can be entered as plain text or a hashed value. SR OS can distinguish between hashed passwords and plain text passwords and take the appropriate action to store the password correctly.</p> <p>"\$2y\$10\$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"</p> <p>For example:</p> <pre>config&gt;system&gt;security# user testuser1 config&gt;system&gt;security&gt;user\$ password "\$2y\$10\$pFoehOg/tCbBMPDJ/ kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK" config&gt;system&gt;security&gt;user# exit config&gt;system&gt;security# info ----- ... user "testuser1" password "\$2y\$10\$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK" exit ...</pre> |

```

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.
- A password value that does not conform to the minimum-length or other password complexity rules can be configured using the **config>system>security>user>password** command, but a warning is provided in the CLI. This allows, for example, an administrator to configure a non-conformant password for a user. A user cannot configure a non-conformant password for themselves using the global **password** 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).

## 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 (either by means of CLI sessions with the file command, '>' redirection, or by means of FTP). 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

## rsa-key

- Syntax** **rsa-key** *public-key-value* *key-id*  
**rsa-key** *key-id*

## User Management Commands

|                    |                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>user                                                                                                                                                                                                                       |
| <b>Description</b> | This command allows the user to associate an RSA public key with the user-name. The public key must be enclosed in quotation marks. This command may be used several times since a user may have multiple public keys. The key is a 1024-bit key. |
| <b>Default</b>     | none                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <i>public-key-value</i> — Specifies the public key up to 255 characters in length. The key is a 1024-bit key.<br><i>key-id</i> — Specifies the key identifier name.                                                                               |
| <b>Values</b>      | 1 — 32                                                                                                                                                                                                                                            |

### snmp

|                    |                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>snmp</b>                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security>user                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command creates the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters.<br><br>All SNMPv3 users must be configured with the commands available in this CLI node.<br><br>The OS always uses the configured SNMPv3 user name as the security user name. |

### user-template

|                    |                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>user-template {tacplus_default   radius_default}</b>                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | This command configures default security user template parameters.                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>tacplus_default</b> — Specifies that the default TACACS+ user template is actively applied to the TACACS+ user.<br><br><b>radius_default</b> — 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

|                    |                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] user user-name</b>                                                                                                                                                                                                           |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                               |
| <b>Description</b> | This command creates a local user and a context to edit the user configuration.<br><br>If a new <i>user-name</i> is entered, the user is created. When an existing <i>user-name</i> is specified, the user parameters can be edited. |



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.

|                   |                                                              |
|-------------------|--------------------------------------------------------------|
| <b>Default</b>    | none                                                         |
| <b>Parameters</b> | <i>user-name</i> — The name of the user up to 32 characters. |

---

## RADIUS Client Commands

### access-algorithm

|                    |                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>access-algorithm {direct   round-robin}</b><br><b>no access-algorithm</b>                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>radius                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command indicates the algorithm used to access the set of RADIUS servers.                                                                                                                                                                                                                                                                                                   |
| <b>Default</b>     | direct                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <p><b>direct</b> — The first server will be used as primary server for all requests, the second as secondary and so on.</p> <p><b>round-robin</b> — 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.</p> |

### accounting

|                    |                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] accounting</b>                                                                                               |
| <b>Context</b>     | config>system>security>radius                                                                                        |
| <b>Description</b> | <p>This command enables RADIUS accounting.</p> <p>The <b>no</b> form of this command disables RADIUS accounting.</p> |
| <b>Default</b>     | no accounting                                                                                                        |

### accounting-port

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

## authorization

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

## interactive-authentication

|                    |                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] authorization</b>                                                                                                                                      |
| <b>Context</b>     | config>system>security>radius                                                                                                                                  |
| <b>Description</b> | This command enables RADIUS interactive authentication for the system. Enabling interactive-authentication forces RADIUS to fall into challenge/response mode. |
| <b>Default</b>     | no authentication                                                                                                                                              |

## port

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

## radius

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

## retry

|                    |                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>retry</b> <i>count</i><br><b>no retry</b>                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>radius<br>config>system>security>dot1x>radius-plcy                                                                                                                                                                   |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | 3                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>count</i> — The retry count.<br><br><b>Values</b> 1 — 10                                                                                                                                                                                 |

## priv-lvl-map

|                    |                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] priv-lvl-map</b>                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                |
| <b>Description</b> | This command is used to specify a series of mappings between TACACS+ priv-lvl and locally configured profiles for authorization. These mappings are used when the use-priv-lvl option is specified for tacplus authorization. |

## priv-lvl

|                    |                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>priv-lvl</b> <i>priv-lvl user-profile-name</i><br><b>no priv-lvl</b> <i>priv-lvl</i>                                                                                                                |
| <b>Context</b>     | config>system>security>tacplus>priv-lvl-map                                                                                                                                                            |
| <b>Description</b> | This command maps a specific TACACS+ priv-lvl to a locally configured profile for authorization. This mapping is used when the <b>use-priv-lvl</b> option is specified for TACPLUS authorization.      |
| <b>Parameters</b>  | <i>priv-lvl</i> — Specifies the privilege level used when sending a TACACS+ ENABLE request.<br><br><b>Values</b> 0 — 15<br><br><i>user-profile-name</i> — Specifies the user profile for this mapping. |

## server

|               |                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>server</b> <i>index address ip-address secret key [hash   hash2]</i><br><b>no server</b> <i>index</i> |
|---------------|----------------------------------------------------------------------------------------------------------|

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>radius                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.</p> <p>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.</p> <p>The <b>no</b> form of the command removes the server from the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Default</b>     | No RADIUS servers are configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <p><i>index</i> — 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.</p> <p><b>Values</b>      1 — 5</p> <p><b>address</b> <i>ip-address</i> — 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.</p> <p><b>Values</b>      ipv4-address      a.b.c.d (host bits must be 0)<br/>                        ipv6-address      x:x:x:x:x:x:x (eight 16-bit pieces)<br/>                                             x:x:x:x:x:d.d.d.d<br/>                                             x: [0..FFFF]H<br/>                                             d: [0..255]D</p> <p><b>secret</b> <i>key</i> — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.</p> <p><b>Values</b>      Up to 128 characters in length.</p> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> 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 <b>hash</b> parameter specified.</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form. If the <b>hash2</b> parameter is not used, the less encrypted <b>hash</b> form is assumed.</p> |

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>radius                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command administratively disables the RADIUS protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.</p> <p>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.</p> <p>The <b>no</b> form of the command administratively enables the protocol which is the default state.</p> |
| <b>Default</b>     | no shutdown                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## timeout

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

## use-default-template

|                    |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] use-default-template</b>                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>radius                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command disables the command.</p> |

## TACACS+ Client Commands

### server

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |               |                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>server</b> <i>index</i> <b>address</b> <i>ip-address</i> <b>secret</b> <i>key</i> [ <b>port</b> <i>port</i> ]<br><b>no server</b> <i>index</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |               |                                                                                                                                                                    |
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |               |                                                                                                                                                                    |
| <b>Description</b> | <p>This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.</p> <p>Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.</p> <p>The <b>no</b> form of the command removes the server from the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |               |                                                                                                                                                                    |
| <b>Default</b>     | No TACACS+ servers are configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |               |                                                                                                                                                                    |
| <b>Parameters</b>  | <p><i>index</i> — The index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.</p> <p><b>Values</b> 1 — 5</p> <p><b>address</b> <i>ip-address</i> — The IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.</p> <table> <tr> <td><b>Values</b></td><td>           ipv4-address      a.b.c.d (host bits must be 0)<br/>           ipv6-address      x:x:x:x:x:x:x:x (eight 16-bit pieces)<br/>                                x:x:x:x:x:x:d.d.d.d<br/>                                x: [0..FFFF]H<br/>                                d: [0..255]D         </td></tr> </table> <p><b>secret</b> <i>key</i> — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.</p> <p><b>Values</b> Up to 128 characters in length.</p> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> 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 <b>hash</b> parameter specified.</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form. If the <b>hash2</b> parameter is not used, the less encrypted <b>hash</b> form is assumed.</p> <p><b>port</b> <i>port</i> — Specifies the port ID.</p> <p><b>Values</b> 0 — 65535</p> | <b>Values</b> | ipv4-address      a.b.c.d (host bits must be 0)<br>ipv6-address      x:x:x:x:x:x:x:x (eight 16-bit pieces)<br>x:x:x:x:x:x:d.d.d.d<br>x: [0..FFFF]H<br>d: [0..255]D |
| <b>Values</b>      | ipv4-address      a.b.c.d (host bits must be 0)<br>ipv6-address      x:x:x:x:x:x:x:x (eight 16-bit pieces)<br>x:x:x:x:x:x:d.d.d.d<br>x: [0..FFFF]H<br>d: [0..255]D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |               |                                                                                                                                                                    |

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.</p> <p>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.</p> <p>The <b>no</b> form of the command administratively enables the protocol which is the default state.</p> |
| <b>Default</b>     | no shutdown                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## tacplus

|                    |                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] tacplus</b>                                                                                                                                                                                                                               |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command creates the context to configure TACACS+ authentication on the router.</p> <p>Configure multiple server addresses for each router for redundancy.</p> <p>The <b>no</b> form of the command removes the TACACS+ configuration.</p> |

## accounting

|                    |                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>accounting [record-type {start-stop   stop-only}]</b><br><b>no accounting</b>                                                                                                                                                                  |
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                                    |
| <b>Description</b> | This command configures the type of accounting record packet that is to be sent to the TACACS+ server. The <b>record-type</b> parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent.         |
| <b>Default</b>     | record-type stop-only                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><b>record-type start-stop</b> — Specifies that a TACACS+ start packet is sent whenever the user executes a command.</p> <p><b>record-type stop-only</b> — Specifies that a stop packet is sent whenever the command execution is complete.</p> |

## authorization

|               |                                          |
|---------------|------------------------------------------|
| <b>Syntax</b> | <b>[no] authorization [use-priv-lvl]</b> |
|---------------|------------------------------------------|



|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command configures TACACS+ authorization parameters for the system.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Default</b>     | no authorization                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                    | <i>use-priv-lvl</i> — Automatically performs a single authorization request to the TACACS+ server for cmd* (all commands) immediately after login, and then use the local profile associated (via the priv-lvl-map) with the priv-lvl returned by the TACACS+ server for all subsequent authorization (except enable-admin). After the initial authorization for cmd*, no further authorization requests will be sent to the TACACS+ server (except enable-admin). |

## interactive-authentication

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] interactive-authentication</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>tacplus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | <p>This configuration instructs SR OS to send no username nor password in the TACACS+ start message, and to display the <i>server_msg</i> in the GETUSER and GETPASS response from the TACACS+ server. Interactive authentication can be used to support a One Time Password scheme (e.g. S/Key). An example flow (e.g. with a telnet connection) is as follows:</p> <ul style="list-style-type: none"> <li>• SR OS will send an authentication start request to the TACACS+ server with no username nor password.</li> <li>• TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETUSER and a <i>server_msg</i>.</li> <li>• SR OS displays the <i>server_msg</i>, and collects the user name.</li> <li>• SR OS sends a continue message with the user name.</li> <li>• TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETPASS and a <i>server_msg</i>.</li> <li>• SR OS displays the <i>server_msg</i> (which may contain, for example, an S/Key for One Time Password operation), and collects the password.</li> <li>• SR OS sends a continue message with the password.</li> <li>• TACACS+ server replies with PASS or FAIL.</li> </ul> |

When interactive-authentication is disabled SR OS will send the username and password in the *tacplus* start message. An example flow (e.g. with a telnet connection) is as follows:

- TAC\_PLUS\_AUTHEN\_TYPE\_ASCII.
  - the login username in the “user” field.
  - the password in the *user\_msg* field (note: this is non-standard but doesn’t cause interoperability problems).
- TACACS+ server ignores the password and replies with TAC\_PLUS\_AUTHEN\_STATUS\_GETPASS.
- SR OS sends a continue packet with the password in the *user\_msg* field.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is enabled, tacplus must be the first method specified in the authentication-order configuration.

**Default** no interactive-authentication

## timeout

**Syntax** **timeout** *seconds*  
**no timeout**

**Context** config>system>security>tacplus

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

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

**Default** 3

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

**Values** 1 — 90

## shutdown

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

**Context** config>system>security>tacplus

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

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

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

**Default** no shutdown

## use-default-template

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

**Context** config>system>security>tacplus

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

---

## Generic 802.1x COMMANDS

### dot1x

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

### radius-plcy

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] radius-plcy</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security> dot1x                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command creates the context to configure RADIUS server parameters for 802.1x network access control on the router.<br><br>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 router as opposed to the RADIUS server configured under the <b>config&gt;system&gt;radius</b> context which authenticates CLI login users who get access to the management plane of the router.<br><br>The <b>no</b> form of the command removes the RADIUS server configuration for 802.1x. |

### retry

|                    |                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>retry count</b><br><b>no retry</b>                                                                                                                                                                                                       |
| <b>Context</b>     | config>system>security> dot1x                                                                                                                                                                                                               |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | 3                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>count</i> — The retry count.<br><br><b>Values</b> 1 — 10                                                                                                                                                                                 |

## server (dot1x)

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>server</b> <i>server-index</i> <b>address</b> <i>ip-address</i> <b>secret</b> <i>key</i> [ <b>hash</b>   <b>hash2</b> ] [ <b>auth-port</b> <i>auth-port</i> ] [ <b>acct-port</b> <i>acct-port</i> ] [ <b>type</b> <i>server-type</i> ]<br><b>no server</b> <i>index</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security> dot1x>radius-plcy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.</p> <p>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.</p> <p>The <b>no</b> form of the command removes the server from the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Default</b>     | No Dot1x servers are configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><i>server-index</i> — 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.</p> <p><b>Values</b> 1 — 5</p> <p><b>address</b> <i>ip-address</i> — 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.</p> <p><b>secret</b> <i>key</i> — The secret key to access the Dot1x server. This secret key must match the password on the Dot1x server.</p> <p><b>Values</b> Up to 128 characters in length.</p> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> 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 <b>hash</b> parameter specified.</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form. If the <b>hash2</b> parameter is not used, the less encrypted <b>hash</b> form is assumed.</p> <p><b>acct-port</b> <i>acct-port</i> — The UDP port number on which to contact the RADIUS server for accounting requests.</p> <p><b>auth-port</b> <i>auth-port</i> — specifies a UDP port number to be used as a match criteria.</p> <p><b>Values</b> 1 — 65535</p> <p><b>type</b> <i>server-type</i> — Specifies the server type.</p> <p><b>Values</b> authorization, accounting, combined</p> |

## source-address

|                    |                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>source-address</b> <i>ip-address</i><br><b>no source-address</b>                                                                            |
| <b>Context</b>     | config>system>security> dot1x>radius-plcy                                                                                                      |
| <b>Description</b> | This command configures the NAS IP address to be sent in the RADIUS packet.<br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | By default the System IP address is used in the NAS field.                                                                                     |
| <b>Parameters</b>  | <i>ip-address</i> — The IP prefix for the IP match criterion in dotted decimal notation.<br><b>Values</b> 0.0.0.0 — 255.255.255.255            |

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>system>security>dot1x<br>config>system>security>dot1x>radius-plcy                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | 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.<br><br>The operational state of the entity is disabled as well as the operational state of any entities contained within.<br><br>The <b>no</b> form of the command administratively enables the protocol which is the default state. |
| <b>Default</b>     | shutdown                                                                                                                                                                                                                                                                                                                                                                                                               |

## timeout

|                    |                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>timeout</b> <i>seconds</i><br><b>no timeout</b>                                                                                                                     |
| <b>Context</b>     | config>system>security> dot1x>radius-plcy                                                                                                                              |
| <b>Description</b> | This command configures the number of seconds the router waits for a response from a RADIUS server.<br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | 3 seconds                                                                                                                                                              |
| <b>Parameters</b>  | <i>seconds</i> — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.<br><b>Values</b> 1 — 90                   |

---

## Keychain Authentication

### keychain

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] keychain</b> <i>keychain-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> 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.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>keychain-name</i> — Specifies a keychain name which identifies this particular keychain entry.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Values</b>      | An ASCII string up to 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### direction

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

### bi

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

### uni

|                |                                           |
|----------------|-------------------------------------------|
| <b>Syntax</b>  | <b>uni</b>                                |
| <b>Context</b> | 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.

## Keychain Authentication

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | There are no default entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b> | <p><i>entry-id</i> — Specifies an entry that represents a key configuration to be applied to a keychain.</p> <p><b>Values</b>      0 — 63</p> <p><b>key</b> — Specifies a key ID which is used along with <i>keychain-name</i> and <b>direction</b> to uniquely identify this particular key entry.</p> <p><i>authentication-key</i> — Specifies the <i>authentication-key</i> that will be used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.</p> <p>The <i>authentication-key</i> can be any combination of letters or numbers. .</p> <p><b>Values</b>      A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.</p> <p><b>algorithm-algorithm</b> — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.</p> <p><b>Values</b>      aes-128-cmac-96 — Specifies an algorithm based on the AES standard for TCP authentication..<br/>hmac-sha-1-96 — Specifies an algorithm based on SHA-1 for RSVP-TE and TCP authentication..<br/>message-digest — MD5 hash used for TCP authentication..<br/>hmac-md5 — MD5 hash used for IS-IS and RSVP-TE..<br/>password — Specifies a simple password authentication for OSPF, IS-IS, and RSVP-TE..<br/>hmac-sha-1 — Specifies the sha-1 algorithm for OSPF, IS-IS, and RSVP-TE..<br/>hmac-sha-256 — Specifies the sha-256 algorithm for OSPF and IS-IS.</p> <p><i>hash-key</i>   <i>hash2-key</i> — The hash key. The key can be any combination of ASCII characters up to 33 for the <i>hash-key</i> and 96 characters for the <i>hash2-key</i> in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).</p> <p>This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.</p> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> 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 <b>hash</b> parameter specified.</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form.</p> |

## begin-time

|                |                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>begin-time</b> [ <i>date</i> ] [ <i>hours-minutes</i> ] [ <b>UTC</b> ] [ <b>now</b> ] [ <b>forever</b> ]                                                                   |
| <b>Context</b> | config>system>security>keychain>direction>bi>entry<br>config>system>security>keychain>direction>uni>receive>entry<br>config>system>security>keychain>direction>uni>send>entry |



|                    |                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.</p> <p>If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.</p> |
| <b>Parameters</b>  | <p><i>date hours-minutes</i> — Specifies the date and time for the key to become active.</p> <p><b>Values</b></p> <p>date: YYYY/MM/DD<br/>hours-minutes: hh:mm[:ss]</p> <p><b>now</b> — Specifies the the key should become active immediately.</p> <p><b>forever</b> — Specifies that the key should always be active.</p>       |

## end-time

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

## tolerance

|                    |                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tolerance</b> [ <i>seconds</i>   <b>forever</b> ]                                                                                                                                                                                           |
| <b>Context</b>     | <pre>config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;send&gt;entry</pre> |
| <b>Description</b> | This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.                                                                                                            |
| <b>Parameters</b>  | <i>seconds</i> — 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.

### option

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>option {basic   isis-enhanced}</b>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>system>security>keychain>direction>bi>entry<br>config>system>security>keychain>direction>uni>send>entry                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | This command configures allows options to be associated with the authentication key.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <b>basic</b> — Specifies that IS-IS should use RFC 5304 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command.<br><br><b>isis-enhanced</b> — Specifies that IS-IS should use RFC 5310 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command. |

### tcp-option-number

|                    |                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-option-number</b>                                                                                   |
| <b>Context</b>     | config>system>security>keychain                                                                            |
| <b>Description</b> | This command enables the context to configure the TCP option number to be placed in the TCP packet header. |

### receive

|                    |                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>receive <i>option-number</i></b>                                                                                                                              |
| <b>Context</b>     | config>system>security>keychain>tcp-option-number                                                                                                                |
| <b>Description</b> | This command configures the TCP option number accepted in TCP packets received.                                                                                  |
| <b>Default</b>     | 254                                                                                                                                                              |
| <b>Parameters</b>  | <i>option-number</i> — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.<br><br><b>Values</b> 253, 254, 253&254 |

## send

|                    |                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>send</b> <i>option-number</i>                                                                                          |
| <b>Context</b>     | config>system>security>keychain>tcp-option-number                                                                         |
| <b>Description</b> | This command configures the TCP option number accepted in TCP packets sent.                                               |
| <b>Default</b>     | 254                                                                                                                       |
| <b>Parameters</b>  | <i>option-number</i> — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header. |
| <b>Values</b>      | 253, 254                                                                                                                  |

---

## CLI Script Commands

### cli-script

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Syntax</b>      | <b>cli-script</b>                                          |
| <b>Context</b>     | config>system>security                                     |
| <b>Description</b> | This command enables the context to configure CLI scripts. |

### authorization

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>authorization</b>                                                |
| <b>Context</b>     | config>system>security>cli-script                                   |
| <b>Description</b> | This command enables the context to authorize CLI script execution. |

### cron

|                    |                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cron</b>                                                                             |
| <b>Context</b>     | config>system>security>cli-script>authorization                                         |
| <b>Description</b> | This command enables the context to configure authorization for the Cron job-scheduler. |

### vsd

|                    |                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] vsd</b>                                                                                                                                                     |
| <b>Context</b>     | config>system>security>cli-script>authorization                                                                                                                     |
| <b>Description</b> | This command enables the context to configure authorization for the VSD server.<br>The <b>no</b> form of the command removes all authorizations for the VSD server. |

### event-handler

|                |                                                 |
|----------------|-------------------------------------------------|
| <b>Syntax</b>  | <b>event-handler</b>                            |
| <b>Context</b> | config>system>security>cli-script>authorization |

**Description** This command enables the context to configure authorization for the Event Handling System (EHS). EHS allows user-controlled programmatic exception handling by allowing a CLI script to be executed upon the detection of a log event.

## cli-user

**Syntax** **cli-user** *user-name*  
**no cli-user**

**Context** config>system>security>cli-script>authorization>event-handler  
 config>system>security>cli-script>authorization>cron  
 config>system>security>cli-script>authorization>vsd

**Description** This command configures The user context under which various types of CLI scripts should execute in order to authorize the script commands. TACACS+ and RADIUS users and authorization are not permitted for **cli-script** authorization.

The **no** form of this command configures scripts to execute with no restrictions and without performing authorization.

**Default** **no cli-user**

**Parameters** *user-name* — The name of a user in the local node database. TACACS+ or RADIUS users can not be used. The user configuration should reference a valid local profile for authorization.

---

## CPM Filter Commands

### cpm-filter

|                    |                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpm-filter</b>                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>system>security                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command disables the CPM filter.</p> |

### default-action

|                    |                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-action {accept   drop}</b>                                                                                                                                                                                       |
| <b>Context</b>     | config>system>security>cpm-filter                                                                                                                                                                                           |
| <b>Description</b> | <p>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.</p> |
| <b>Default</b>     | accept                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <p><b>accept</b> — Specifies that packets matching the filter entry are forwarded.</p> <p><b>drop</b> — Specifies that packets matching the filter entry are dropped.</p>                                                   |

### ip-filter

|                    |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] ip-filter</b>                                                          |
| <b>Context</b>     | config>system>security>cpm-filter                                              |
| <b>Description</b> | <p>This command enables the context to configure CPM IP filter parameters.</p> |
| <b>Default</b>     | shutdown                                                                       |
| <b>Description</b> |                                                                                |

### mac-filter

|               |                        |
|---------------|------------------------|
| <b>Syntax</b> | <b>[no] mac-filter</b> |
|---------------|------------------------|

|                    |                                                                          |
|--------------------|--------------------------------------------------------------------------|
| <b>Context</b>     | config>system>security>cpm-filter                                        |
| <b>Description</b> | This command enables the context to configure CPM MAC-filter parameters. |
| <b>Default</b>     | shutdown                                                                 |

## entry

|                    |                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>entry</b> <i>entry-id</i>                                                                                                                                                                                      |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter<br>config>sys>sec>cpm>mac-filter                                                                                                                                                     |
| <b>Description</b> | This command specifies a particular CPM filter match entry. Every CPM filter must have at least one filter match entry. Entries are created and deleted by user.<br><br>The default match criteria is match none. |
| <b>Parameters</b>  | <i>entry-id</i> — Identifies a CPM filter entry as configured on this system.                                                                                                                                     |
| <b>Values</b>      | 1 — 2048                                                                                                                                                                                                          |
| <b>Description</b> |                                                                                                                                                                                                                   |

## log

|                    |                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>log</b> <i>log-id</i>                                                                                                                                                                               |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry<br>config>sys>sec>cpm>mac-filter>entry                                                                                                                              |
| <b>Description</b> | This command specifies the log in which packets matching this entry should be entered. The value zero indicates that logging is disabled.<br><br>The <b>no</b> form of the command deletes the log ID. |
| <b>Parameters</b>  | <i>log-id</i> — Specifies the log ID where packets matching this entry should be entered.                                                                                                              |

## match

|                    |                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>match</b> [ <b>protocol</b> <i>protocol-id</i> ]<br><b>no match</b>                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | 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, hexadecimal, 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 10: 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                                    |
| 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          | OSPF-IGP                                                    |
| ether-ip    | 97          | Ethernet-within-IP Encapsulation                            |
| encap       | 98          | Encapsulation Header                                        |



**Table 10: IP Protocol Names (Continued)**

| Protocol | Protocol ID | Description                        |
|----------|-------------|------------------------------------|
| 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                     |
| crtip    | 126         | Combat Radio Transport Protocol    |
| crudp    | 127         | Combat Radio User Datagram         |

**Description****dscp**

|                    |                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dscp</b> <i>dscp-name</i><br><b>no dscp</b>                                                                                                                                      |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match<br>config>sys>sec>cpm>mac-filter>entry>match                                                                                               |
| <b>Description</b> | This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.<br><br>The <b>no</b> form of the command removes the DSCP match criterion.    |
| <b>Default</b>     | <b>no dscp</b> — No dscp match criterion.                                                                                                                                           |
| <b>Parameters</b>  | <i>dscp-name</i> — Configures a dscp name that has been previously mapped to a value using the <b>dscp-name</b> command. The DiffServ code point may only be specified by its name. |

**dst-ip**

|                    |                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-ip</b> <i>ipv6-address/prefix-length</i><br><b>dst-ip ipv6-prefix-list</b> <i>ipv6-prefix-list-name</i><br><b>no dst-ip</b>                                                                                                                                                           |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command configures a destination IP address range to be used as an IP filter match criterion.<br><br>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

**ip-prefix-list** — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

*ip-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

*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-port

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

**Context** config>sys>sec>cpm>ip-filter>entry>match

**Description** This command specifies the TCP/UDP port or port name to match the destination-port of the packet. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

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

**Parameters** *tcp/udp port-numb-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)

*port-list-name* — Specifies the port list name to be used as a match criteria for the destination port.

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

**Values** [0x0000..0xFFFF] | [0..65535] | [0b0000000000000000..0b1111111111111111]

## fragment

**Syntax** **fragment** {true | false}  
**no fragment**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match<br>config>sys>sec>cpm>ipv6-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.</p> <p>This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The no version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.</p> <p>The <b>no</b> form of the command removes the match criterion.</p> <p>This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The no version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.</p> |
| <b>Default</b>     | <b>no fragment</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <p><b>true</b> — Specifies to match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value. For IPv6, packet matches if it contains IPv6 Fragmentation Extension Header.</p> <p><b>false</b> — Specifies to match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero. For IPv6, packet matches if it does not contain IPv6 Fragmentation Extension Header.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## icmp-code

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>icmp-code</b> <i>icmp-code</i><br><b>no icmp-code</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>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 Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.</p> <p>The behavior of the <b>icmp-code</b> value is dependent on the configured <b>icmp-type</b> value, thus a configuration with only an <b>icmp-code</b> value specified will have no effect. To match on the <b>icmp-code</b>, an associated <b>icmp-type</b> must also be specified.</p> <p>The <b>no</b> form of the command removes the criterion from the match entry.</p> |
| <b>Default</b>     | <b>no icmp-code</b> - no match criterion for the ICMP code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <p><i>icmp-code</i> — Specifies the ICMP code values that must be present to match.</p> <p><b>Values</b>      0 — 255</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## icmp-type

|                    |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>icmp-type</b> <i>icmp-type</i><br><b>no icmp-type</b>                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match<br>config>sys>sec>cpm>ipv6-filter>entry>match                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | 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 Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.<br><br>The <b>no</b> form of the command removes the criterion from the match entry. |
| <b>Default</b>     | <b>no icmp-type</b> — No match criterion for the ICMP type.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>icmp-type</i> — Specifies the ICMP type values that must be present to match.<br><br><b>Values</b> 0 — 255                                                                                                                                                                                                                                                                                                 |

## ip-option

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-option</b> <i>ip-option-value ip-option-mask</i><br><b>no ip-option</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | 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.<br><br>The option-type octet contains 3 fields: <ul style="list-style-type: none"> <li>• 1 bit copied flag (copy options in all fragments)</li> <li>• 2 bits option class,</li> <li>• 5 bits option number.</li> </ul> The <b>no</b> form of the command removes the match criterion.                                                                                                                                                  |
| <b>Default</b>     | No IP option match criterion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>ip-option-value</i> — 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.<br><br>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).<br><br><b>Values</b> 0 — 255<br><br><i>ip-option-mask</i> — 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 |
| <b>Default</b> | 255 (decimal) (exact match) |           |
| <b>Values</b>  | 1 — 255 (decimal)           |           |

## multiple-option

|                    |                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>multiple-option {true   false}</b><br><b>no multiple-option</b>                                                                                                                                                                                                      |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                |
| <b>Description</b> | This command configures matching packets that contain more than one option fields in the IP header as an IP filter match criterion.<br><br>The <b>no</b> form of the command removes the checking of the number of option fields in the IP header as a match criterion. |
| <b>Default</b>     | <b>no multiple-option</b> — No checking for the number of option fields in the IP header                                                                                                                                                                                |
| <b>Parameters</b>  | <b>true</b> — Specifies matching on IP packets that contain more that one option field in the header.<br><b>false</b> — Specifies matching on IP packets that do not contain multiple option fields present in the header.                                              |

## option-present

|                    |                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>option-present {true   false}</b><br><b>no option-present</b>                                                                                                                                                                                                                  |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                          |
| <b>Description</b> | 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.<br><br>The <b>no</b> 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.

## src-ip

- Syntax** **src-ip** [*ip-address/mask* | **ip-prefix-list** *prefix-list-name*]  
**no src-ip**
- Context** config>sys>sec>cpm>ip-filter>entry>match
- Description** This command specifies the IP address to match the source IP 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 1010:0:0:0:700:0:217A.
- |               |                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Values</b> | ipv4-address      a.b.c.d (host bits must be 0)<br>x:x:x:x:x:d.d.d.d[-interface]<br>x: [0..FFFF]H<br>d: [0..255]D<br>interface: 32 characters maximum, mandatory for link local addresses<br><br>mask:                Specifies the 16 bit mask to be applied when matching the source IP address.<br>1 — 32 |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- ip-prefix-list** — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.
- ip-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

### Description

## src-port

- Syntax** **src-port** *src-port-number* [*mask*]

|                    |                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                                |
| <b>Description</b> | This command specifies the TCP/UDP port to match the source port of the packet. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.        |
| <b>Parameters</b>  | <p><i>src-port-number</i> — The source port number to be used as a match criteria expressed as a decimal integer.</p> <p><b>Values</b>      0 — 65535</p> <p><i>mask</i> — Specifies the 16 bit mask to be applied when matching the source port.</p> <p><b>Values</b>      0 — 128</p> |

## tcp-ack

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-ack {true   false}</b><br><b>no tcp-ack</b>                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>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 Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.</p> <p>The <b>no</b> form of the command removes the criterion from the match entry.</p> |
| <b>Default</b>     | No match criterion for the ACK bit                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><b>true</b> — 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.</p> <p><b>false</b> — 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.</p>                                                                                                                                         |

## tcp-syn

|                    |                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-syn {true   false}</b><br><b>no tcp-syn</b>                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>sys>sec>cpm>ip-filter>entry>match<br>config>sys>sec>cpm>ipv6-filter>entry>match<br>config>sys>sec>cpm>ipv6-filter>entry>match                                                                                                                                                                                                                               |
| <b>Description</b> | 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 Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. |

The 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

**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>mac-filter>entry>match

### Description

**Description** This command renumbers existing IP(IPv4), IPv6, or MAC 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

## shutdown

**Syntax** **shutdown**

**Context** config>sys>sec>cpm>ip-filter  
config>sys>sec>cpm>ipv6-filter  
config>sys>sec>cpm>mac-filter

**Description** This command enables IP(v4) or MAC CPM filter.

The **no** form of this command disable the filter.

**Default** shutdown



---

## CPM Queue Commands

### cpm-queue

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpm-queue</b>                                           |
| <b>Context</b>     | config>system>security                                     |
| <b>Description</b> | This command enables the context to configure a CPM queue. |

### queue

|                    |                                                      |
|--------------------|------------------------------------------------------|
| <b>Syntax</b>      | <b>queue</b> <i>queue-id</i>                         |
| <b>Context</b>     | config>system>security>cpm-queue                     |
| <b>Description</b> | This command allows users to allocate dedicated CPM. |

### cbs

|                    |                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cbs</b> <i>cbs</i><br><b>no cbs</b>                                                                                     |
| <b>Context</b>     | config>system>cpm-queue>queue                                                                                              |
| <b>Description</b> | This command specifies the amount of buffer that can be drawn from the reserved buffer portion of the queue's buffer pool. |
| <b>Parameters</b>  | <i>cbs</i> — Specifies the committed burst size in kbytes.                                                                 |

### mbs

|                    |                                                                           |
|--------------------|---------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mbs</b> <i>mbs</i><br><b>no mbs</b>                                    |
| <b>Context</b>     | config>system>security>cpm-queue>queue                                    |
| <b>Description</b> | This command specifies the maximum queue depth to which a queue can grow. |
| <b>Parameters</b>  | <i>mbs</i> — Specifies the maximum burst size in kbytes.                  |

### rate

|                    |                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rate</b> <i>rate</i> [ <b>cir</b> <i>cir</i> ]<br><b>no rate</b>                                                                                                        |
| <b>Context</b>     | config>system>security>cpm-queue>queue                                                                                                                                     |
| <b>Description</b> | This command specifies the maximum bandwidth that will be made available to the queue in kilobits per second (kbps).                                                       |
| <b>Parameters</b>  | <i>rate</i> — Specifies the administrative Peak Information Rate (PIR) for the queue.<br><b>cir</b> <i>cir</i> — Specifies the amount of bandwidth committed to the queue. |

---

## TTL Security Commands

### ttl-security

|                    |                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ttl-security</b> <i>min-ttl-value</i><br><b>no ttl-security</b>                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>router>bgp>group<br>config>router>bgp>group>neighbor<br>configure>router>ldp>peer-parameters>peer<br>config>system>login-control>ssh<br>config>system>login-control>telnet                                                                                                                                                                                                                            |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command disables TTL security. |
| <b>Parameters</b>  | <i>min-ttl-value</i> — Specify the minimum TTL value for an incoming BGP packet.<br><br><b>Values</b> 1 — 255                                                                                                                                                                                                                                                                                                |

### ttl-security

|                    |                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ttl-security</b> <i>min-ttl-value</i><br><b>no ttl-security</b>                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>router>ldp>peer-parameters>peer                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command disables TTL security. |
| <b>Default</b>     | no ttl-security                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <i>min-ttl-value</i> — Specifies the minimum TTL value for an incoming LDP packet.<br><br><b>Values</b> 1 — 255                                                                                                                                                                                                                                                                                              |

### ttl-security

|               |                                          |
|---------------|------------------------------------------|
| <b>Syntax</b> | <b>ttl-security</b> <i>min-ttl-value</i> |
|---------------|------------------------------------------|

### **no ttl-security**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>system>login-control>ssh<br>config>system>login-control>telnet                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>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.</p> <p>The <b>no</b> form of the command disables TTL security.</p> |
| <b>Parameters</b>  | <i>min-ttl-value</i> — Specify the minimum TTL value for an incoming BGP packet.                                                                                                                                                                                                                                                                                                                                           |
| <b>Values</b>      | 1 — 255                                                                                                                                                                                                                                                                                                                                                                                                                    |

---

## CPU Protection Commands

### cpu-protection

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b>                                                   |
| <b>Context</b>     | config>sys>security                                                     |
| <b>Description</b> | This command enters the context to configure CPU protection parameters. |

### included-protocols

|                    |                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>included-protocols</b>                                                                                                                                           |
| <b>Context</b>     | config>sys>security>cpu-protection> ip>included-protocols                                                                                                           |
| <b>Description</b> | This context allows configuration of which protocols are included for ip-src-monitoring. This is system-wide configuration that applies to cpu protection globally. |

### dhcp

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] dhcp</b>                                                                                                                                |
| <b>Context</b>     | config>sys>security>cpu-protection> ip>included-protocols                                                                                       |
| <b>Description</b> | Include extracted IPv4 DHCP packets for ip-src-monitoring. IPv4 DHCP packets will be subject to the per-source-rate of cpu protection policies. |
| <b>Default</b>     | dhcp (note this is different than the other protocols)                                                                                          |

### gtp

|                    |                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] gtp</b>                                                                                                                               |
| <b>Context</b>     | config>sys>security>cpu-protection> ip>included-protocols                                                                                     |
| <b>Description</b> | Include extracted IPV4 GTP packets for ip-src-monitoring. IPv4 GTP packets will be subject to the per-source-rate of cpu protection policies. |
| <b>Default</b>     | no gtp                                                                                                                                        |

## icmp

|                |                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>[no] icmp</b>                                                                                                                                                                                             |
| <b>Context</b> | config>sys>security>cpu-protection> ip>included-protocols<br>Include extracted IPv4 ICMP packets for ip-src-monitoring. IPv4 ICMP packets will be subject to the per-source-rate of cpu protection policies. |
| <b>Default</b> | no icmp                                                                                                                                                                                                      |

## igmp

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] igmp</b>                                                                                                                                |
| <b>Context</b>     | config>sys>security>cpu-protection> ip>included-protocols                                                                                       |
| <b>Description</b> | Include extracted IPv4 IGMP packets for ip-src-monitoring. IPv4 IGMP packets will be subject to the per-source-rate of cpu protection policies. |
| <b>Default</b>     | no igmp                                                                                                                                         |

## link-specific-rate

|                    |                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>link-specific-rate</b> <i>packet-rate-limit</i><br><b>no link-specific-rate</b>                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>sys>security>cpu-protection                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | 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. |
| <b>Default</b>     | max (no limit)                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>packet-rate-limit</i> — Specifies a packet arrival rate limit, in packets per second, for link level protocols.                                                                                                                                                                                                        |
| <b>Values</b>      | 1 — 65535, max (no limit)                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>     | 15000                                                                                                                                                                                                                                                                                                                     |

## policy

|                |                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>policy</b> <i>cpu-protection-policy-id</i> <b>[create]</b><br><b>no policy</b> <i>cpu-protection-policy-id</i> |
| <b>Context</b> | config>sys>security>cpu-protection                                                                                |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command configures CPU protection policies.</p> <p>The <b>no</b> form of the command deletes the specified policy from the configuration.</p> <p>Policies 254 and 255 are reserved as the default access and network interface policies, and cannot be deleted. The parameters within these policies can be modified. An event will be logged (warning) when the default policies are modified.</p>                                                                                                                                                                    |
| <b>Default</b>     | <p>Policy 254 (default access interface policy):</p> <p style="padding-left: 40px;">per-source-rate: max (no limit)</p> <p style="padding-left: 40px;">overall-rate : 6000</p> <p style="padding-left: 40px;">out-profile-rate: 6000</p> <p style="padding-left: 40px;">alarm</p> <p>Policy 255 (default network interface policy):</p> <p style="padding-left: 40px;">per-source-rate: max (no limit)</p> <p style="padding-left: 40px;">overall-rate : max (no limit)</p> <p style="padding-left: 40px;">out-profile-rate: 3000</p> <p style="padding-left: 40px;">alarm</p> |
| <b>Parameters</b>  | <p><i>cpu-protection-policy-id</i> — Assigns a policy ID to the specific CPU protection policy.</p> <p><b>Values</b>      1 — 255</p> <p><b>create</b> — Keyword used to create CPU protection policy. The <b>create</b> keyword requirement can be enabled/disabled in the <b>environment&gt;create</b> context.</p>                                                                                                                                                                                                                                                          |

## alarm

|                    |                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] alarm</b>                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>sys>security>cpu-protection>policy                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command enables the generation of an event when a rate is exceeded. The event includes information about the offending source. Only one event is generated per monitor period.</p> <p>The <b>no</b> form of the command disables the notifications.</p> |
| <b>Default</b>     | no alarm                                                                                                                                                                                                                                                        |

## eth-cfm

|                |                                           |
|----------------|-------------------------------------------|
| <b>Syntax</b>  | <b>eth-cfm</b><br><b>no eth-cfm</b>       |
| <b>Context</b> | config>sys>security>cpu-protection>policy |

|                    |                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | 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. |
| <b>Default</b>     | None                                                                                                                                                                                                               |

## entry

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>entry</b> <entry> <b>levels</b> <levels> <b>opcodes</b> <opcodes> <b>rate</b> <packet-rate-limit><br><b>no entry</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>sys>security>cpu-protection>eth-cfm>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | Builds the specific match and rate criteria. Up to ten entries may exist in up to four CPU protection policies.<br><br>The <b>no</b> form of the command reverses the match and rate criteria configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Default</b>     | no entry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <b>rate</b> — Specifies a packet rate limit in frames per second, where a '0' means drop all.<br><br><b>Values</b> 1 —100<br><br><b>level</b> — Specifies a domain level.<br><br><b>Values</b> all                      Wildcard entry level<br>range                  0 —7: within specified range, multiple ranges allowed<br>number                0 ... 7: specific level number, may be combined with range<br><br><b>opcode</b> — Specifies an operational code that identifies the application.<br><br><b>Values</b> range                  0 —255: within specified range, multiple ranges allowed<br>number                0 .. 255: specific level number, may be combined with range |

## out-profile-rate

|                    |                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>out-profile-rate</b> packet-rate-limit [log-event]<br><b>no out-profile-rate</b>                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>sys>security>cpu-protection>policy                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command applies a packet arrival rate limit for the entire SAP/interface, above which packets will be marked as discard eligible. The rate defined is a global rate limit for the interface regardless of the number of traffic flows. It is a per-SAP/interface rate.<br><br>The <b>no</b> form of the command sets out-profile-rate parameter back to the default value. |
| <b>Default</b>     | <b>3000</b> for cpu-protection-policy-id 1-253<br><b>6000</b> for cpu-protection-policy-id 254 (default access interface policy)<br><b>3000</b> for cpu-protection-policy-id 255 (default network interface policy)                                                                                                                                                             |



|                   |                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>packet-rate-limit</i> — Specifies a packet arrival rate limit in packets per second.                                                                                                                                                    |
| <b>Values</b>     | 1 — 65535, max (max indicates no limit)                                                                                                                                                                                                    |
| <b>log-events</b> | — issues a <i>tmnxCpmProtViolSapOutProf</i> , <i>tmnxCpmProtViolIfOutProf</i> , or <i>tmnxCpmProtViolSdpBindOutProf</i> log event and tracks violating interfaces when the out-profile-rate is exceeded. Supported on CPM3 and above only. |

## overall-rate

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>overall-rate</b> <i>packet-rate-limit</i><br><b>no overall-rate</b>                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>sys>security>cpu-protection>policy                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>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 traffic flows are present on the SAP/interface. It is a per-SAP/interface rate.</p> <p>The <b>no</b> form of the command sets overall-rate parameter back to the default value.</p> |
| <b>Default</b>     | <b>max</b> for cpu-protection-policy-id 1 — 253<br><b>6000</b> for cpu-protection-policy-id 254 (default access interface policy)<br><b>max</b> for cpu-protection-policy-id 255 (default network interface policy)                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>packet-rate-limit</i> — Specifies a packet arrival rate limit in packets per second.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Values</b>      | 1 — 65535, max (max indicates no limit)                                                                                                                                                                                                                                                                                                                                                                                                       |

## per-source-rate

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>per-source-rate</b> <i>packet-rate-limit</i><br><b>no per-source-rate</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>sys>security>cpu-protection>policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | <p>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 (<i>mac-monitoring</i>) or SAP and source IP address (<i>ip-src-monitoring</i>). The CPU will receive no more than the configured packet rate from each source (only certain protocols are rate limited for <i>ip-src-monitoring</i> as configured under ‘include-protocols’ in the <i>cpu protection</i> policy). The measurement is cleared each second.</p> <p>This parameter is only applicable if the policy is assigned to an interface (some examples include <i>saps</i>, <i>subscriber-interfaces</i>, and <i>spoke-sdps</i>), and the <b>mac-monitor</b> or <b>ip-src-monitor</b> keyword is specified in the <b>cpu-protection</b> configuration of that interface.</p> <p>The <i>ip-src-monitoring</i> is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios, all packets from all subscribers</p> |

behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

|                   |                                                                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | max, no limit                                                                                                                                                |
| <b>Parameters</b> | <i>packet-rate-limit</i> — Specifies a per-source packet (per SAP/MAC source address or per SAP/IP source address) arrival rate limit in packets per second. |
| <b>Values</b>     | 1 — 65535, max (max indicates no limit)                                                                                                                      |

## port-overall-rate

|                    |                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port-overall-rate</b> <i>packet-rate-limit</i> [ <b>low-action-priority</b> ]<br><b>no port-overall-rate</b>                                                                                      |
| <b>Context</b>     | config>sys>security>cpu-protection                                                                                                                                                                   |
| <b>Description</b> | This command configures a per-port overall rate limit for CPU protection.                                                                                                                            |
| <b>Parameters</b>  | <i>packet-rate-limit</i> — Specifies an overall per-port packet arrival rate limit in packets per second.                                                                                            |
| <b>Values</b>      | 1 — 65535, max (indicates no limit)                                                                                                                                                                  |
|                    | <b>action-low-priority</b> — Marks packets that exceed the rate as low-priority (for preferential discard later if there is congestion in the control plane) instead of discarding them immediately. |
| <b>Default</b>     | max                                                                                                                                                                                                  |

## protocol-protection

|                    |                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>protocol-protection</b> [ <b>allow-sham-links</b> ] [ <b>block-pim-tunneled</b> ]<br><b>no protocol-protection</b>                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>sys>security>cpu-protection                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | 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. |
| <b>Default</b>     | no protocol-protection                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b>  | <b>allow-sham-links</b> — Allows sham links. As OSPF sham links form an adjacency over the MPLS-VPNN backbone network, when protocol-protection is enabled, the tunneled OSPF packets to be received over the backbone network must be explicitly allowed.                                                                                                                                            |
|                    | <b>block-pim-tunneled</b> — - Blocks extraction and processing of PIM packets arriving at the SR-OS node inside a tunnel (for example, MPLS or GRE) on a network interface. With protocol-protection enabled and tunneled pim blocked, PIM in an mVPN on the egress DR will not switch traffic from the (*,G) to the (S,G) tree.                                                                      |

## cpu-protection

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b> <i>policy-id</i><br><b>no cpu-protection</b>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>router>interface<br>config>service>ies>interface<br>config>service>ies>video-interface<br>config>service>vpls>video-interface<br>config>service>vprn>interface<br>config>service>vprn>network-interface<br>config>service>vprn>video-interface                                                                                                                                                                                                                                                   |
| <b>Description</b> | <p>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.</p> <p>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.</p> <p>The <b>no</b> form of the command reverts to the default values.</p> |
| <b>Default</b>     | <p>cpu-protection 254 (for access interfaces)</p> <p>cpu-protection 255 (for network interfaces)</p> <p>none (for video-interfaces, shown as no cpu-protection in CLI)</p> <p>The configuration of <b>no cpu-protection</b> returns the interface to the default policies as shown above.</p>                                                                                                                                                                                                           |

## cpu-protection

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b> <i>policy-id</i> [ <b>mac-monitoring</b> ] [ <b>ip-src-monitoring</b> ]<br><b>no cpu-protection</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>subscriber-mgmt>msap-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>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.</p> <p>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.</p> <p>The <b>no</b> form of the command reverts to the default values.</p> |
| <b>Default</b>     | <p>cpu-protection 254 (for access interfaces)</p> <p>cpu-protection 255 (for network interfaces)</p> <p>The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.</p>                                                                                                                                                                                                                                                                                                                                                             |

- 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 certain protocol packets using the per-source-rate and included-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

## cpu-protection

- Syntax** **cpu-protection** *policy-id* [**mac-monitoring**][**eth-cfm-monitoring** [**aggregate**][**car**]] [**ip-src-monitoring**]  
**no cpu-protection**
- Context** config>service>ies>interface>sap  
 config>service>ies>interface>spoke-sdp  
 config>service>ies>sub-if>grp-if>sap  
 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 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 certain protocol packets using the per-source-rate and include-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.
  - 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.

## cpu-protection

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b> <i>policy-id</i> [ <b>mac-monitoring</b> ][ <b>eth-cfm-monitoring</b> [ <b>aggregate</b> ][ <b>car</b> ]]<br><b>no cpu-protection</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>service>epipe>sap<br>config>service>epipe>spoke-sdp<br>config>service>ipipe>sap<br>config>service>template>vpls-sap-template<br>config>service>vpls>mesh-sdp<br>config>service>vpls>sap<br>config>service>vpls>spoke-sdp                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>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.</p> <p>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.</p> <p>The <b>no</b> form of the command reverts to the default values.</p> |
| <b>Default</b>     | <p>cpu-protection 254 (for access interfaces)</p> <p>cpu-protection 255 (for network interfaces)</p> <p>The configuration of <b>no cpu-protection</b> returns the SAP/SDP/template to the default policies as shown above.</p>                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b>  | <p><b>mac-monitoring</b> — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.</p> <p><b>eth-cfm-monitoring</b> — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP/SDP/template.</p> <p><b>aggregate</b> — applies the rate limit to the sum of the per-peer packet rates.</p> <p><b>car</b> — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.</p>                                                                                                                         |

---

## Distributed CPU Protection Commands

### dist-cpu-protection

|                    |                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dist-cpu-protection</b>                                                                             |
| <b>Context</b>     | config>system>security                                                                                 |
| <b>Description</b> | This command enters the CLI context for configuration of the Distributed CPU Protection (DCP) feature. |

### policy

|                    |                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] policy</b> <i>policy-name</i>                                                                                                                            |
| <b>Context</b>     | config>system>security>dist-cpu-protection                                                                                                                       |
| <b>Description</b> | This command configures one of the maximum 16 Distributed CPU Protection policies. These policies can be applied to objects such as SAPs and network interfaces. |
| <b>Parameters</b>  | <i>policy-name</i> — Name of the policy to be configured.                                                                                                        |

### description

|                |                                                   |
|----------------|---------------------------------------------------|
| <b>Syntax</b>  | <b>[no] description</b> <i>string</i>             |
| <b>Context</b> | config>system>security>dist-cpu-protection>policy |

### rate

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rate kbps</b> <i>kilobits-per-second max</i> [ <b>mbs size</b> ] [ <b>bytes kilobytes</b> ]<br><b>rate packets</b> <i>{ppi max}</i> <b>within seconds</b> [ <b>initial-delay packets</b> ]<br><b>no rate</b>                                                                                                                                                                                                                              |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>static-policer<br>config>system>security>dist-cpu-protection>policy>local-monitoring-policer<br>config>system>security>dist-cpu-protection>policy>protocol>dynamic-parameters                                                                                                                                                                                                              |
| <b>Description</b> | This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.<br><br>The actual hardware may not be able to perfectly rate limit to the exact configured parameters. In this case, the configured parameters will be adapted to the closest supported rate. The actual (operational) parameters can be seen in CLI, for example, “show service id 33 sap 1/1/3:33 dist-cpu-protection detail”. |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | rate packets max within 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b> | <p><b>packets kbps</b> — specifies that the rate is either in units of packets per interval or in units of kilobits-per-second. The packets option would typically be used for lower rates (for example, for per subscriber DHCP rate limiting) while the kbps option would typically be used for higher rates (for example, per interface BGP rate limiting).</p> <p><b>ppi</b> — Specifies packets per interval. 0..255 or max (0 = all packets are non-conformant)</p> <ul style="list-style-type: none"> <li>• rate of max=effectively disable the policier (always conformant)</li> <li>• rate of packets 0 = all packets considered non-conformant.</li> </ul> <p><b>within seconds</b> — Specifies the length of the ppi rate measurement interval.</p> <p><b>Values</b> 1..32767</p> <p><b>initial-delay packets</b> — The number of packets allowed (even at line rate) in an initial burst (or a burst after the policer bucket has drained to zero) in addition to the normal “ppi”. This would typically be set to a value that is equal to the number of received packets in several full handshakes/negotiations of the particular protocol.</p> <p><b>Values</b> 1..255</p> <p><b>kbps kilobits-per-second</b> —</p> <p><b>Values</b> 1..2000000 max max = This effectively disable the policer (always conformant).</p> <p><b>mbs</b> — =The tolerance for the kbps rate</p> <p><b>Values</b> 0..4194304. A configured mbs of 0 will cause all packets to be considered non-conformant.</p> <p><b>bytes kilobytes</b> — Specifies that the units of the mbs size parameter are either in bytes or kilobytes.</p> <p><b>Default</b> The default mbs sets the mbs to 10ms of the kbps.</p> |

## detection-time

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>detection-time seconds</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>static-policer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | When a policer is declared as in an “exceed” state, it will remain as exceeding until a contiguous conformant period of <b>detection-time</b> passes. The <b>detection-time</b> only starts after the exceed-action hold-down is complete. If the policer detects another exceed during the detection count down then a hold-down is once again triggered before the policer re-enters the detection time (that is, the countdown timer starts again at the configured value). During the hold-down (and the detection-time), the policer is considered as in an “exceed” state. |
| <b>Default</b>     | 30                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><b>seconds</b> — Specifies in seconds.</p> <p><b>Values</b> 1..128000</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## dynamic-enforcement-policer-pool

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] dynamic-enforcement-policer-pool</b> <i>number-of-policers</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>dist-cpu-protection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command reserves a set of policers for use as dynamic enforcement policers for the Distributed CPU Protection (DCP) feature. Policers are allocated from this pool and instantiated as per-object-per-protocol dynamic enforcement policers after a local monitor is triggered for an object (such as a SAP or Network Interface). Any change to this configured value automatically clears the high water mark, timestamp, and failed allocation counts as seen under “show card x fp y dist-cpu-protection” and in the tmnxFpDcpDynEnfrcPlcrStatTable in the TIMETRA-CHASSIS-MIB. Decreasing this value to below the currently used/allocated number causes all dynamic policers to be returned to the free pool (and traffic returns to the local monitors). |
| <b>Default</b>     | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <i>number-of-policers</i> — specifies the number of policers to be reserved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Values</b>      | 0, 1000..32k                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## exceed-action

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>exceed-action {discard [hold-down seconds]   low-priority [hold-down seconds]   none}</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>static-policer<br>config>system>security>dist-cpu-protection>policy>protocol>dynamic-parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <p><b>discard</b> — Discards packets that are non-conformant.</p> <p><b>low-priority</b> — Marks packets that are non-conformant as low-priority. If there is congestion in the control plane of the SR OS router then unmarked control packets are given preferential treatment.</p> <p><b>hold-down seconds</b> — (optional) When the parameter is specified, it causes the following “hold-down” behavior.</p> <p>When SR OS software detects that an enforcement policer has marked or discarded one or more packets (software may detect this some time after the packets are actually discarded), and an optional <b>hold-down seconds</b> value has been specified for the <b>exceed-action</b>, then the policer will be set into a “mark-all” or “drop-all” mode that cause the following:</p> <ul style="list-style-type: none"> <li>- the policer state to be updated as normal</li> <li>- all packets to be marked (if the action is “low-priority”) or dropped (action = discard) regardless of the results of the policing decisions/actions/state.</li> </ul> |



The **hold-down** is cleared after approximately the configured time in seconds after it was set. The **hold-down seconds** option should be selected for protocols that receive more than one packet in a complete handshake/negotiation (for example, DHCP, PPP). **hold-down** is not applicable to a local monitoring policer. The “detection-time” will only start after any **hold-down** is complete. During the **hold-down** (and the detection-time), the policer is considered as in an “exceed” state. The policer may re-enter the hold-down state if an exceed packet is detected during the detection-time countdown. The allowed values are [none|1..10080|indefinite].

**Values** 1-10080 in seconds

**none** — no hold-down

**indefinite** — hold down is in place until the operator clears it manually using a tools command (tools perform security dist-cpu-protection release-hold-down) or removes the dist-cpu-protection policy from the object.

## exceed-action

|                    |                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>exceed-action {discard   low-priority   none}</b>                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>local-monitoring-policer                                                                                                                                                                                                                                              |
| <b>Description</b> | This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.                                                                                                                                                                                           |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <p><b>discard</b> — Discards packets that are non-conformant.</p> <p><b>low-priority</b> — Marks packets that are non-conformant as low-priority. If there is congestion in the control plane of the SR OS router then unmarked control packets are given preferential treatment.</p> <p><b>none</b> — no hold-down</p> |

## log-events

|                    |                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] log-events [verbose]</b>                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>static-policer                                                                                                                                                                |
| <b>Description</b> | This command controls the creation of log events related to static-policer status and activity.                                                                                                                                 |
| <b>Default</b>     | <p>default = log-events</p> <p>log-events: send the Exceed (Excd) and Conform events (e.g. sapDcpStaticExcd)</p>                                                                                                                |
| <b>Parameters</b>  | <b>verbose</b> — (optional) Sends the same events as just “log-events” plus Hold Down Start and Hold Down End events. The optional “verbose” includes some events that are more likely used during debug/tuning/investigations. |

## local-monitoring-policer

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] local-monitoring-policer <i>policer-name</i> [create]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>local-monitoring-policer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>This command configures a monitoring policier that is used to monitor the aggregate rate of several protocols arriving on an object (for example, SAP). When the <b>local-monitoring-policer</b> is determined to be in a non-conformant state (at the end of a minimum monitoring time of 60 seconds) then the system will attempt to allocate dynamic policers for the particular object for any protocols associated with the local monitor (for example, via the “protocol xyz enforcement” CLI command).</p> <p>If the system cannot allocate all the dynamic policers within 150 seconds, it will stop attempting to allocate dynamic policers, raise a LocMonExcdAllDynAlloc log event, and go back to using the local monitor. The local monitor may then detect exceeded packets again and make another attempt at allocating dynamic policers.</p> <p>Once this <i>policer-name</i> is referenced by a protocol then this policer will be instantiated for each “object” that is created and references this DDoS policy. If there is no policer free then the object will be blocked from being created.</p> |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies name of the policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Values</b>      | [32 chars max]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## log-events

|                    |                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] log-events [verbose]</b>                                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>local-monitoring-policer                                                                                                                                                                                      |
| <b>Description</b> | This command controls the creation of log events related to <b>local-monitoring-policer</b> status and activity.                                                                                                                                                |
| <b>Default</b>     | log-events: send the DcpLocMonExcdOutOfDynRes events                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>verbose</b> — This parameter sends the same events as just “log-events” plus DcpLocMonExcd, DcpLocMonExcdAllDynAlloc, and DcpLocMonExcdAllDynFreed. The optional “verbose” includes some events that are more likely used during debug/tuning/investigations |

## protocol

|                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] protocol <i>name</i> [create]</b>                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command creates the protocol for control in the policy.</p> <p>Control packets that are both forwarded (which means they could be subject to normal QoS policy policing) and also copied for extraction are not subject to distributed cpu protection (including in the all-unspecified bucket). This includes traffic snooping (for example, PIM in VPLS) as well as con-</p> |

trol traffic that is flooded in an R-VPLS instance and also extracted to the CPM such as ARP, ISIS and VRRP. Centralized per SAP/interface cpu-protection can be employed to rate limit or mark this traffic if desired.

Explanatory notes for some of the protocols:

- bfd-cpm: includes all bfd handled on the CPM including cpm-np type, single hop and multi-hop, and MPLS-TP CC and CV bfd
- dhcp: includes dhcp for IPv4 and IPv6
- eth-cfm: 802.1ag and includes Y.1731. Eth-cfm packets on port and LAG based facility MEPs are not included (but packets on Tunnel MEPs are).
- icmp: includes IPv4 and IPv6 ICMP except Neighbor Discovery which is classified as a separate protocol 'ndis'
- isis: includes isis used for SPBM
- ldp: includes ldp and t-ldp
- mpls-ttl: MPLS packets that are extracted due to an expired mpls ttl field
- ndis: IPv6 Neighbor Discovery
- ospf: includes all OSPFv2 and OSPFv3 packets.
- pppoe-pppoa: includes PADx, LCP, PAP/CHAP and NCPs
- all-undefined: a special 'protocol'. When configured, this treats all extracted control packets that are not explicitly created in the dist-cpu-protection policy as a single aggregate flow (or "virtual protocol"). It lumps together "all the rest of the control traffic" to allow it to be rate limited as one flow. It includes all control traffic of all protocols that are extracted and sent to the CPM (even protocols that cannot be explicitly configured with the distributed cpu protection feature). Control packets that are both forwarded and copied for extraction are not included. If an operator later explicitly configures a protocol, then that protocol is suddenly no longer part of the "all-undefined" flow. The "all-undefined" protocol must be explicitly configured in order to operate.

"no protocol x" means packets of protocol x are not monitored and not enforced (although they do count in the fp protocol queue) on the objects to which this dist-cpu-protection policy is assigned, although the packets will be treated as part of the all-undefined protocol if the all-undefined protocol is created in the policy.

|                   |                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | none                                                                                                                     |
| <b>Parameters</b> | <i>names</i> — Signifies protocol name.                                                                                  |
| <b>Values</b>     | arp dhcp http-redirect icmp igmp mld ndis pppoe-pppoa all-undefined mpls-ttl bfd-cpm bgp eth-cfm isis ldp ospf pim rsvp. |

## enforcement

|                |                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>enforcement</b> {static <i>policer-name</i>   dynamic { <i>mon-policer-name</i>   local-mon-bypass}} |
| <b>Context</b> | config>system>security>dist-cpu-protection>policy>protocols                                             |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command configures the enforcement method for the protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default</b>     | dynamic local-mon-bypass                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <b>static</b> — the protocol is always enforced using a static-policer. Multiple protocols can reference the same static-policer. Packets of protocols that are statically enforced bypass any local monitors.<br><i>policer name</i> — Specifies the name is a static-policer.<br><b>dynamic</b> — A specific enforcement policer for this protocol for this SAP/object is instantiated when the associated local-monitoring-policer is determined to be in a non-conformant state (at the end of a minimum monitoring time of 60 seconds to reduce thrashing).<br><i>mon-policer-name</i> — Specifies which local-monitoring-policer to use<br><b>local-mon-bypass</b> — This parameter is used to not include packets from this protocol in the local monitoring function, and when the local-monitor “trips”, do not instantiate a dynamic enforcement policer for this protocol. |

### detection-time

|                    |                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>detection-time</b> <i>seconds</i>                                                                                                               |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>protocols>dynamic-parameters                                                                     |
| <b>Description</b> | When a dynamic enforcing policer is instantiated, it will remain allocated until at least a contiguous conformant period of detection-time passes. |

### dynamic-parameters

|                    |                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dynamic-parameters</b>                                                                                                                                                                                                                          |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>protocols                                                                                                                                                                                        |
| <b>Description</b> | The dynamic-parameters are used to instantiate a dynamic enforcement policer for the protocol when the associated local-monitoring-policer is considered as exceeding its rate parameters (at the end of a minimum monitoring time of 60 seconds). |

### log-events

|                    |                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] log-events [verbose]</b>                                                                          |
| <b>Context</b>     | config>system>security>dist-cpu-protection>policy>protocols>dynamic-parameters                            |
| <b>Description</b> | This command controls the creation of log events related to dynamic enforcement policer status & activity |
| <b>Default</b>     | log-events - send the Exceed (Excd) and Conform events                                                    |

**Parameters**     **verbose** — This parameter sends the send the same events as just “log-events” plus Hold Down Start, Hold Down End, DcpDynamicEnforceAlloc and DcpDynamicEnforceFreed events. The optional “verbose” includes the allocation/de-allocation events (typically used for debug/tuning only – could be very noisy even when there is nothing much of concern).

## static-policer

**Syntax**     **[no] static-policer policer-name [create]**

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

**Description**     Configures a static enforcement policer that can be referenced by one or more protocols in the policy. Once this policer-name is referenced by a protocol, then this policer will be instantiated for each object (e.g. SAP or network interface) that is created and references this policy. If there is no policer resource available on the associated card/fp then the object will be blocked from being created. Multiple protocols can use the same static-policer.

**Parameters**     *policy-name* — Specifies the name of the policy.

**Values**     [32 chars max]



---

## Show Commands

---

### Security Commands

---

#### access-group

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

**Table 11: 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
snmp-ro snmpv2c none no-security
snmp-rw snmpv1 none no-security no-security
snmp-rw snmpv2c none 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 12: 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.<br>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#
*A:Dut-C# show system security authentication statistics

=====
Authentication sequence : radius tacplus local
=====
type status timeout single retry
server address (secs) conn count

health check : enabled (interval 30)

=====
Login Statistics
=====
server address conn accepted rejected
 errors logins logins

local n/a 4 0

=====
Authorization Statistics (TACACS+)
=====
server address conn sent rejected
 errors pkts pkts

=====
Accounting Statistics
=====
server address conn sent rejected
 errors pkts pkts

=====
```

communities

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

**Table 13: 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.<br>rw — The community string allows read-write access.<br>rwa — The community string allows read-write access.<br>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**

|                    |                                    |
|--------------------|------------------------------------|
| <b>Syntax</b>      | <b>cpm-filter</b>                  |
| <b>Context</b>     | show>system>security               |
| <b>Description</b> | This command displays CPM filters. |

## ip-filter

|                    |                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-filter</b> [ <b>entry</b> <i>entry-id</i> ]                                          |
| <b>Context</b>     | show>system>security>cpm-filter                                                            |
| <b>Description</b> | This command displays CPM IP filters.                                                      |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Identifies a CPM filter entry as configured on this system. |
|                    | <b>Values</b> 1 — 2048                                                                     |
| <b>Output</b>      | <b>CPM Filter Output</b> — The following table describes CPM IP filter output fields..     |

**Table 14: 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 or prefix-list)                       |
| 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.                              |
| 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. |

**Table 14: Show CPM IP Filter Output Fields (Continued)**

| Label          | Description                                    |
|----------------|------------------------------------------------|
| 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** `ipv6-filter [entry entry-id]`
- Context** `show>system>security>cpm-filter`
- Description** This command displays CPM IPv6 filters.
- Parameters** `entry entry-id` — Identifies a CPM filter entry as configured on this system.
- Values** 1 — 2048

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 15: 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 : 10000000
CBS : 4096 MBS : 8192
=====
A:ALA-35#
```

## cpu-protection

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b>                                                   |
| <b>Context</b>     | show>system>security                                                    |
| <b>Description</b> | 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<br>First-Time | Level<br>Last-Time  | OpCode | 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 30000000007
1:2 3
 255 max 05/01/2010 01:43:55 06/27/2010 22:37:23 30000000008
1:3 3
 100 61234 05/01/2010 01:43:57 06/27/2010 22:37:26 30000000009
1:4 3
 255 max 05/01/2010 01:43:59 06/27/2010 22:37:29 30000000010
1:5 3
 100 61234 05/01/2010 01:44:01 06/27/2010 22:37:32 30000000011

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
=====

```

## eth-cfm-monitoring

|                    |                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>eth-cfm-monitoring</b> [{ <i>service-id service-id sap-id sap-id</i> }   { <i>service-id service-id sdp-id sdp-id:vc-id</i> }] |
| <b>Context</b>     | show>system>security>cpu-protection                                                                                               |
| <b>Description</b> | This command displays sources exceeding their eth-cfm-monitoring rate limit.                                                      |

## dist-cpu-protection

|                    |                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dist-cpu-protection</b>                                                                                         |
| <b>Context</b>     | show>card>fp                                                                                                       |
| <b>Description</b> | This command displays Distributed CPU Protection parameters and status at the per card and forwarding plane level. |

**Output****Table 16: Show Distributed CPU Protection Output Fields**

| Label                                  | Description                                                                                                                                                                                                                                                                                       |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Card                                   | The card identifier                                                                                                                                                                                                                                                                               |
| Forwarding Plane (FP)                  | Identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, an IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMA's).                                                            |
| Dynamic Enforcement Policer Pool       | The configured size of the dynamic-enforcement-policer-pool for this card/FP.                                                                                                                                                                                                                     |
| Dynamic-Policers Currently In Use      | The number of policers from the dynamic enforcement policer pool that are currently in use. The policers are allocated from the pool and instantiated as per-object-per-protocol dynamic enforcement policers after a local monitor triggered for an object (such as a SAP or Network Interface). |
| Hi-WaterMark Hit Count                 | The maximum Currently In Use value since it was last cleared (clear card x fp y dist-cpu-protection)                                                                                                                                                                                              |
| Hi-WaterMark Hit Time                  | The time at which the current Hi-WaterMark Hit Count was first recorded.                                                                                                                                                                                                                          |
| Dynamic-Policers Allocation Fail Count | Indicates how many times the system attempted to allocate dynamic enforcement policers but could not get enough the fill the request.                                                                                                                                                             |

```
*A:nodeA# show card 1 fp 1 dist-cpu-protection
```

```
=====
Card : 1 Forwarding Plane(FP) : 1
=====
Dynamic Enforcement Policer Pool : 2000

Statistics Information

Dynamic-Policers Currently In Use : 48
Hi-WaterMark Hit Count : 72
Hi-WaterMark Hit Time : 01/03/2013 15:08:42 UTC
Dynamic-Policers Allocation Fail Count : 0

=====
```

## dist-cpu-protection

|                    |                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dist-cpu-protection [detail]</b>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | show>service>id>sap                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | This command displays Distributed CPU Protection parameters and status at the per SAP level.                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b>  | <b>detail</b> — Include the adapted operational rate parameters in the CLI output. The adapted Oper. parameters are only applicable if the policer is instantiated (for example, if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed. |
| <b>Output</b>      | <b>Distributed CPU Protection Policer Output</b> — The following table describes Distributed CPU Protection Policer Output output fields.                                                                                                                                                                                                                                                                   |

**Table 17: Show Distributed CPU Protection Policer Output Fields**

| Label                             | Description                                                                                                                                                                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Distributed CPU Protection Policy | The DCP policy assigned to the object.                                                                                                                                                                                                                             |
| Policer-Name                      | The configured name of the static policer                                                                                                                                                                                                                          |
| Card/FP                           | The card and FP identifier. FP identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMA's). |
| Policer-State                     | The state of the policer with the following potential values:                                                                                                                                                                                                      |

**Table 17: Show Distributed CPU Protection Policer Output Fields (Continued)**

| Label            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p><i>Exceed</i> - The policer has been detected as non-conformant to the associated DCP policy parameters (e.g. packets exceeded the configured rate and the DCP polling process identified this occurrence)</p> <p><i>Conform</i> - The policer has been detected as conformant to the associated DCP policy parameters (rate)</p> <p><i>not-applicable</i> - Newly created policers or policers that are not currently instantiated. This includes policers configured on linecards that are not in service.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Protocols Mapped | A list of protocols that are configured to map to the particular policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Oper. xyz fields | <p>The actual hardware may not be able to perfectly rate limit to the exact configured rate parameters in a DCP policy. In this case the configured rate parameters will be adapted to the closest supported rate. These adapted operational values are displayed in CLI when the “detail” keyword is included in the show command. The adapted Oper. parameters are only applicable if the policer is instantiated (e.g. if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed.</p> <p><i>Oper. Kbps</i> - The adapted ‘kilobits-per-second’ value for DCP ‘kbps’ rates</p> <p><i>Oper. MBS</i> - The adapted ‘mbs size’ value for DCP ‘kbps’ rates</p> <p><i>Oper. Depth</i> - The calculated policer bucket depth in packets (for DCP ‘packets’ rates) or in bytes (for DCP ‘kbps’ rates)</p> <p><i>Oper. Packets</i> - The adapted ‘ppi’ value for DCP ‘packets’ rates</p> <p><i>Oper. Within</i> - The adapted ‘within seconds’ value for DCP ‘packets’ rates</p> <p><i>Oper. Init. Delay</i> - The adapted ‘initial-delay packets’ value for DCP ‘packets’ rates</p> |
| Exceed-Count     | The count of packets exceeding the policing parameters since the given policer was previously declared as conformant or newly instantiated. This counter has the same behavior as the exceed counter in the DCP the log events – they are baselined (reset) when the policer transitions to conformant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 17: Show Distributed CPU Protection Policer Output Fields (Continued)**

| Label               | Description                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Detec. Time Remain  | The remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it is once again conformant. |
| Hold-Down Remain    | The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.                                              |
| All Dyn-Plcr Alloc. | Indicates that all the dynamic enforcement policers have been allocated and instantiated for a given local-monitor.                                     |
| Dyn-Policer Alloc.  | Indicates that a dynamic policer has been instantiated.                                                                                                 |

**Sample Output**

```
*A:nodeA# show service id 33 sap 1/1/3:33 dist-cpu-protection detail

=====
Service Access Points(SAP) 1/1/3:33
=====
Distributed CPU Protection Policy : test1

Statistics/Policer-State Information
=====

Static Policer

Policer-Name : arp
Card/FP : 1/1
Protocols Mapped : arp
Exceed-Count : 0
Detec. Time Remain : 0 seconds
Operational (adapted) rate parameters:
 Oper. Packets : 5 ppi
 Oper. Initial Delay: 6 packets
 Oper. Depth : 0 packets
Policer-State : Conform
Hold-Down Remain. : none
Oper. Within : 8 seconds

Policer-Name : dhcp
Card/FP : 1/1
Protocols Mapped : dhcp
Exceed-Count : 0
Detec. Time Remain : 0 seconds
Operational (adapted) rate parameters:
 Oper. Kbps : 2343 kbps
 Oper. Depth : 0 bytes
Policer-State : Conform
Hold-Down Remain. : none
Oper. MBS : 240 kilobytes

... (snip)

*A:nodaA# show service id 33 sap 1/1/3:34 dist-cpu-protection detail
```



```

=====
Service Access Points(SAP) 1/1/3:34
=====
Distributed CPU Protection Policy : test2

Statistics/Policer-State Information
=====

Static Policer

No entries found

Local-Monitoring Policer

Policer-Name : my-local-mon1
Card/FP : 1/1
Protocols Mapped : arp, pppoe-pppoa
Exceed-Count : 0
All Dyn-Plcr Alloc. : False
Operational (adapted) rate parameters:
 Oper. Packets : 10 ppi
 Oper. Initial Delay: 8 packets
 Oper. Depth : 0 packets
 Oper. Within : 8 seconds

Dynamic-Policer (Protocol)

Protocol(Dyn-Plcr) : arp
Card/FP : 1/1
Exceed-Count : 0
Detec. Time Remain : 0 seconds
Dyn-Policer Alloc. : False
Operational (adapted) rate parameters: unknown
Protocol-State : not-applicable
Hold-Down Remain. : none

Protocol(Dyn-Plcr) : pppoe-pppoa
Card/FP : 1/1
Exceed-Count : 0
Detec. Time Remain : 0 seconds
Dyn-Policer Alloc. : False
Operational (adapted) rate parameters: unknown
Protocol-State : not-applicable
Hold-Down Remain. : none

```

## dist-cpu-protection

|                    |                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dist-cpu-protection [detail]</b>                                                                   |
| <b>Context</b>     | show>router>interface                                                                                 |
| <b>Description</b> | This command displays Distributed CPU Protection parameters and status at the router Interface level. |

- Parameters**     **detail** — Include the adapted operational rate parameters in the CLI output. The adapted Oper. parameters are only applicable if the policer is instantiated (for example, if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed.
- Output**     **Distributed CPU Protection Policer Output** — The following table describes Distributed CPU Protection Policer Output output fields.

**Table 18: Show Distributed CPU Protection Policer Output Fields**

| Label                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Distributed CPU Protection Policy | The DCP policy assigned to the object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Policer-Name                      | The configured name of the static policer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Card/FP                           | The card and FP identifier. FP identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMA's).                                                                                                                                                                                                                                                                                                                                                                                |
| Policer-State                     | The state of the policer with the following potential values:<br><br><i>Exceed</i> - The policer has been detected as non-conformant to the associated DCP policy parameters (e.g. packets exceeded the configured rate and the DCP polling process identified this occurrence)<br><br><i>Conform</i> - The policer has been detected as conformant to the associated DCP policy parameters (rate)<br><br><i>not-applicable</i> - Newly created policers or policers that are not currently instantiated. This includes policers configured on linecards that are not in service.                                                                 |
| Protocols Mapped                  | A list of protocols that are configured to map to the particular policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Oper. xyz fields                  | The actual hardware may not be able to perfectly rate limit to the exact configured rate parameters in a DCP policy. In this case the configured rate parameters will be adapted to the closest supported rate. These adapted operational values are displayed in CLI when the “detail” keyword is included in the show command. The adapted Oper. parameters are only applicable if the policer is instantiated (e.g. if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed. |

**Table 18: Show Distributed CPU Protection Policer Output Fields (Continued)**

| Label               | Description                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <i>Oper. Kbps</i> - The adapted 'kilobits-per-second' value for DCP 'kbps' rates                                                                                                                                                                                                                        |
|                     | <i>Oper. MBS</i> - The adapted 'mbs size' value for DCP 'kbps' rates                                                                                                                                                                                                                                    |
|                     | <i>Oper. Depth</i> - The calculated policer bucket depth in packets (for DCP 'packets' rates) or in bytes (for DCP 'kbps' rates)                                                                                                                                                                        |
|                     | <i>Oper. Packets</i> - The adapted 'ppi' value for DCP 'packets' rates                                                                                                                                                                                                                                  |
|                     | <i>Oper. Within</i> - The adapted 'within seconds' value for DCP 'packets' rates                                                                                                                                                                                                                        |
|                     | <i>Oper. Init. Delay</i> - The adapted 'initial-delay packets' value for DCP 'packets' rates                                                                                                                                                                                                            |
| Exceed-Count        | The count of packets exceeding the policing parameters since the given policer was previously declared as conformant or newly instantiated. This counter has the same behavior as the exceed counter in the DCP the log events – they are baselined (reset) when the policer transitions to conformant. |
| Detec. Time Remain  | The remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it is once again conformant.                                                                                                                                                 |
| Hold-Down Remain    | The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.                                                                                                                                                                                              |
| All Dyn-Plcr Alloc. | Indicates that all the dynamic enforcement policers have been allocated and instantiated for a given local-monitor.                                                                                                                                                                                     |
| Dyn-Policer Alloc.  | Indicates that a dynamic policer has been instantiated.                                                                                                                                                                                                                                                 |

**Sample Output**

```
*A:Dut-A# show router interface "test" dist-cpu-protection detail
```

```
=====
Interface "test" (Router: Base)
=====
Distributed CPU Protection Policy : dcpuPol

Statistics/Policer-State Information
```

```

=====

Static Policer

Policer-Name : staticArpPolicer
Card/FP : 4/1 Policer-State : Exceed
Protocols Mapped : arp
Exceed-Count : 10275218
Detec. Time Remain : 29 seconds Hold-Down Remain. : none
Operational (adapted) Rate Parameters:
 Oper. Packets : 100 ppi Oper. Within : 1 seconds
 Oper. Initial Delay: none
 Oper. Depth : 100 packets

Local-Monitoring Policer

Policer-Name : localMonitor
Card/FP : 4/1 Policer-State : Exceed
Protocols Mapped : icmp, ospf
Exceed-Count : 8019857
All Dyn-Plcr Alloc. : True
Operational (adapted) Rate Parameters:
 Oper. Packets : 200 ppi Oper. Within : 1 seconds
 Oper. Initial Delay: none
 Oper. Depth : 0 packets

Dynamic-Policer (Protocol)

Protocol (Dyn-Plcr) : icmp
Card/FP : 4/1 Protocol-State : Exceed
Exceed-Count : 1948137
Detec. Time Remain : 29 seconds Hold-Down Remain. : none
Dyn-Policer Alloc. : True
Operational (adapted) Rate Parameters:
 Oper. Kbps : 25 kbps Oper. MBS : 256 bytes
 Oper. Depth : 274 bytes

Protocol (Dyn-Plcr) : ospf
Card/FP : 4/1 Protocol-State : Exceed
Exceed-Count : 1487737
Detec. Time Remain : 29 seconds Hold-Down Remain. : none
Dyn-Policer Alloc. : True
Operational (adapted) Rate Parameters:
 Oper. Kbps : 25 kbps Oper. MBS : 256 bytes
 Oper. Depth : 284 bytes

=====

```

## excessive-sources

|                    |                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>excessive-sources</b> [ <b>service-id</b> <i>service-id</i> <b>sap-id</b> <i>sap-id</i> ]                                                                                                                         |
| <b>Context</b>     | show>system>security>cpu-protection                                                                                                                                                                                  |
| <b>Description</b> | This command displays sources exceeding their per-source rate limit.                                                                                                                                                 |
| <b>Parameters</b>  | <b>service-id</b> <i>service-id</i> — Displays information for services exceeding their per-source rate limit.<br><b>sap-id</b> <i>sap-id</i> — Displays information for SAPs exceeding their per-source rate limit. |

## policy

|                    |                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>policy</b> [ <i>policy-id</i> ] <b>association</b>                                                                                                            |
| <b>Context</b>     | show>system>security>cpu-protection<br>show>system>security>dist-cpu-protection                                                                                  |
| <b>Description</b> | This command displays CPU protection policy information.                                                                                                         |
| <b>Parameters</b>  | <i>policy-id</i> — Displays CPU protection policy information for the specified policy ID><br><b>association</b> — This keyword displays policy-id associations. |

## protocol-protection

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>protocol-protection</b>                                       |
| <b>Context</b>     | show>system>security>cpu-protection                              |
| <b>Description</b> | This command display all interfaces with non-zero drop counters. |

## violators

|                    |                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>violators</b> [ <b>port</b> ] [ <b>interface</b> ] [ <b>sap</b> ] [ <b>video</b> ] [ <b>sdp</b> ]                                                                                                                                                                                             |
| <b>Context</b>     | show>system>security>cpu-protection                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command displays all interfaces, ports or SAPs with CPU protection policy violators. It also includes objects (saps, interfaces) that exceed the out-profile-rate and have the log-events keyword enabled for the out-profile-rate in the cpu-protection policy associated with the object. |
| <b>Parameters</b>  | <b>port</b> — Displays violators associated with the port.<br><b>interface</b> — Displays violators associated with the interface.<br><b>sap</b> — Displays violators associated with the SAP.<br><b>video</b> — Displays violators associated with the video entity.                            |

**sdp** — Displays violators associated with the SDP.

### Sample Output

```
*A:SecuritySR7>config>sys>security>cpu-protection>policy# 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

toIxia Base
 255 1000 10/02/2012 18:38:23 10/02/2012 18:39:31 70

1 interface(s) found
=====

=====
SAP's where the protection policy overall rate limit is violated
=====
SAP-Id Service-Id
 Plcy Limit First-Time Last-Time Violation-Periods

No 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

No 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
=====
```

## mac-filter

|                    |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mac-filter</b> [ <b>entry</b> <i>entry-id</i> ]                             |
| <b>Context</b>     | show>system>security>cpm-filter                                                |
| <b>Description</b> | This command displays CPM MAC filters.                                         |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Displays information about the specified entry. |
| <b>Values</b>      | 1 — 2048                                                                       |

## Sample Output

```
*B:bksim67# show system security cpm-filter mac-filter
=====
CPM Mac Filter (applied)
=====
Entry-Id Dropped Forwarded Description

1 23002 47094

Num CPM Mac filter entries: 1
=====
*B:bksim67#
```

## mac-filter

|                    |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mac-filter</b> [ <b>entry</b> <i>entry-id</i> ]                             |
| <b>Context</b>     | show>system>security>management-access-filter                                  |
| <b>Description</b> | This command displays management access MAC filters.                           |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Displays information about the specified entry. |
| <b>Values</b>      | 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

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

## Sample Output

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



```

Active : No Tolerance : 500
Begin Time : 2007/02/15 18:28:13 Begin Time (UTC) : 2007/02/15 17:28:13
End Time : 2007/02/15 18:28:37 End Time (UTC) : 2007/02/15 17:28:37
=====
*A:ALA-A#

```

## management-access-filter

**Syntax**     **management-access-filter**

**Context**    show>system>security

**Description** This command displays management access filter information for IP and MAC filters.

## ip-filter

**Syntax**     **ip-filter** [**entry** *entry-id*]

**Context**    show>system>security>mgmt-access-filter

**Description** This command displays management-access IP filters.

**Parameters** *entry-id* — Displays information for the specified entry.

**Values**     1 — 9999

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

**Table 19: Show Management Access Filter Output Fields**

| Label       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Def. action | <p>Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted.</p> <p>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.</p> <p>Deny-host-unreachble — Specifies that packets not matching the configured selection criteria in the filter entries are denied.</p> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                      |

**Table 19: Show Management Access Filter Output Fields (Continued)**

| Label         | Description                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------|
| Src interface | The interface name for the next hop to which the packet should be forwarded if it hits this filter entry. |
| Dest port     | The destination port.                                                                                     |
| Matches       | The number of times a management packet has matched this filter entry.                                    |
| Protocol      | The IP protocol to match.                                                                                 |
| Action        | The action to take for packets that match this filter entry.                                              |

```
*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#
```

## password-options

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

**Table 20: Show Password Options 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. |

**Table 20: Show Password Options Output Fields (Continued)**

| <b>Label</b>                                   | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time required between password changes         | Displays the time interval between changed passwords.                                                                                                                                                                                                                                                                                                                       |
| Number of invalid attempts permitted per login | Displays the number of unsuccessful login attempts allowed for the specified <b>time</b> .                                                                                                                                                                                                                                                                                  |
| 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 number of minutes that the user is locked out if the threshold of unsuccessful login attempts has been exceeded.                                                                                                                                                                                                                                               |
| Authentication order                           | Displays the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords.                                                                                                                                                                                                                                                             |
| User password history length                   | Displays the size of the password history file to be stored.                                                                                                                                                                                                                                                                                                                |
| Accepted password length                       | Displays the minimum length required for local passwords.                                                                                                                                                                                                                                                                                                                   |
| Credits for each character type                | Displays the credit for each character type. A credit is obtained for a particular character type; for example, uppercase, lowercase, numeric, or special character. Credits per character type are configurable. Credits can be used towards the minimum length of the password, so a trade-off can be made between a very long, simple password and a short, complex one. |
| Required character types                       | Displays the character types that are required in a password; for example, uppercase, lowercase, numeric, or special character.                                                                                                                                                                                                                                             |
| Minimum number different character types       | Displays the minimum number of each different character types in a password.                                                                                                                                                                                                                                                                                                |
| Required distance with previous password       | Displays the minimum Levenshtein distance between a new password and the old password.                                                                                                                                                                                                                                                                                      |
| Allow consecutively repeating a character      | Displays the number of times the same character is allowed to be repeated consecutively.                                                                                                                                                                                                                                                                                    |
| Allow passwords containing user-name           | Displays whether the user name is allowed as part of the password.                                                                                                                                                                                                                                                                                                          |
| Palindrome allowed                             | Displays whether palindromes are allowed as part of the password.                                                                                                                                                                                                                                                                                                           |

**Sample Output**

```

A:ALA-7# show system security password-options

=====
Password Options
=====

Password aging in days : none
Time required between password changes : 0d 00:10:00

Number of invalid attempts permitted per login : 3
Time in minutes per login attempt : 5
Lockout period (when threshold breached) : 10
Authentication order : radius tacplus local
User password history length : disabled
Accepted password length : 6..56 characters
Credits for each character type : none
Required character types : none
Minimum number different character types : 0
Required distance with previous password : 5
Allow consecutively repeating a character : always
Allow passwords containing username : yes
Palindrome allowed : no
=====
A:ALA-7#

```

**per-peer-queuing**

|                    |                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>per-peer-queuing</b>                                                                                                         |
| <b>Context</b>     | show>system>security                                                                                                            |
| <b>Description</b> | This command enables or disables CPMCFM hardware queuing per peer. TTL security only operates when per-peer-queuing is enabled. |
| <b>Output</b>      | <b>Per-Peer-Queuing Output</b> — The following table describes per-peer-queuing output fields.                                  |

**Table 21: 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** [*user-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** *user-profile-name* — Displays information for the specified user profile.
- Output** **User Profile Output** — The following table describes user profile output fields.

**Table 22: 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.<br>Deny — Denies access to all commands.<br>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.<br>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**

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

**Table 23: Show Source Address Output Fields**

| Label                        | Description                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------------------|
| Application                  | Displays the source-address application.                                                         |
| IP address<br>Interface Name | Displays the source address IP address or interface name.                                        |
| Oper status                  | Up — The source address is operationally up.<br>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. The type of SSH application (CLI, SCP, SFTP or NETCONF) is indicated for each SSH connection.

**Output**        **SSH Options Output** — The following table describes SSH output fields .

| Label                  | Description                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH status             | SSH is enabled — Displays that SSH server is enabled.<br>SSH is disabled — Displays that SSH server is disabled.                                                                                                                                   |
| SSH Preserve Key       | Enabled — Displays that preserve-key is enabled.<br>Disabled — Displays that preserve-key is disabled.                                                                                                                                             |
| SSH protocol version 1 | Enabled — Displays that SSH1 is enabled.<br>Disabled — Displays that SSH1 is disabled.                                                                                                                                                             |
| SSH protocol version 2 | Enabled — Displays that SSH2 is enabled.<br>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.<br>3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.                                                                                  |
| Username               | The name of the user.                                                                                                                                                                                                                              |
| Version                | The SSH version number.                                                                                                                                                                                                                            |
| Server Name            | The type of SSH application (CLI, SCP, SFTP or NETCONF)                                                                                                                                                                                            |
| Number of SSH sessions | The total number of SSH sessions.                                                                                                                                                                                                                  |

## Sample output

```
*A:ALA-49# show system security ssh
```

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

SSH Protocol Version 1 : Disabled

SSH Protocol Version 2 : Enabled
DSA Host Key Fingerprint : 88:41:1c:7e:97:64:df:a0:e4:54:c2:cc:3d:dd:c7:70
RSA Host Key Fingerprint : 63:b8:c4:8a:17:b7:1c:95:35:91:c9:08:75:cc:31:a3

Connection Username Version ServerName Status

138.120.214.254 admin 2 netconf connected
138.120.140.148 admin 2 cli connected

Number of SSH sessions : 2
=====
```



## user

- Syntax** **user** [*user-id*] [**detail**]  
**user** [*user-id*] **lockout**
- 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.  
**lockout** — Displays information about any users who are currently locked out.
- 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.<br>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.<br>N — The user does not have the ability to change the login password.                                                                                                                                                                                                   |
| User permissions | Console — Y - The user is authorized for console access.<br>N- The user is not authorized for console access.<br><br>FTP — Y - The user is authorized for FTP access.<br>N - The user is not authorized for FTP access.<br><br>SNMP — Y - The user is authorized for SNMP access.<br>N - The user is not authorized for SNMP access. |
| Password expires | The number of days in which the user must change his login password.                                                                                                                                                                                                                                                                 |
| Attempted logins | The number of times the user has attempted to login irrespective of whether the login succeeded or failed.                                                                                                                                                                                                                           |
| Failed logins    | The number of unsuccessful login attempts.                                                                                                                                                                                                                                                                                           |
| Local conf       | Y — Password authentication is based on the local password database.<br>N — Password authentication is not based on the local password database.                                                                                                                                                                                     |
| Home directory   | Specifies the local home directory for the user for both console and FTP access.                                                                                                                                                                                                                                                     |

| Label              | Description (Continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restricted to home | <p>Yes — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device.</p> <p>No — The user is allowed to navigate to a directory higher in the directory tree on the home directory device.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Login exec file    | <p>Displays the user's login exec file which executes whenever the user successfully logs in to a console session.</p> <p>profile - the security profile(s) associated with the user</p> <p>locked-out - no / yes (time remaining). Indicates the the user is currently locked-out. After the time expires, or the lockout is manually cleared, the user will be able to attempt to log into the node again.</p> <p>Remaining Login attempts - number of login attempts remaining until the user will be locked-out</p> <p>Remaining Lockout Time - The time until the lockout is automatically cleared and the user can attempt to log into the node again.</p> |

### 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#
*A:Dut-C# show system security user detail
=====
Users
=====
User ID New User Permissions Password Login Failed Local
 Pwd console ftp li snmp Expires Attempts Logins Conf

admin n y n n n never 4 0 y

Number of users : 1
=====

*A:Dut-C# show system security user detail
=====
User Configuration Detail
=====
user id : admin

console parameters

new pw required : no cannot change pw : no
home directory :
restricted to home : no
login exec file :
profile : administrative
locked-out : yes (9:23 remaining)

snmp parameters
=====

*A:Node234# show system security user lockout
=====
Currently Failed Login Attempts
=====
User ID Remaining Login attempts Remaining Lockout Time (min:sec)

jason123 N/A 9:56

Number of users : 1
=====

```

With the introduction of the PKI on an SR (SSH Server) the authentication process can be done via PKI or password. SSH client usually authenticate via PKI and password if PKI is configured on the client. In this case PKI takes precedence over password in most clients.

All client authentications are logged and display in the **show>system>security>user detail**. [Table 24](#) shows the rules where pass and fail attempts are logged.

Table 24: Pass/Fail Login Attempts

| Authentica-<br>tion Order | Client<br>(i.e., putty)   | Server<br>(i.e., SR)                                               |                        | CLI<br>Show System Security<br>Attempts (SR) |                  |
|---------------------------|---------------------------|--------------------------------------------------------------------|------------------------|----------------------------------------------|------------------|
|                           | Private Key<br>Programmed | Public Key<br>Configured                                           | Password<br>Configured | Logins<br>Attempts                           | Failed<br>Logins |
| 1. Public Key             | Yes                       | Yes                                                                | N/A                    | Increment                                    |                  |
| 2. Password               | Yes                       | Yes (No match<br>between client<br>and server. Go to<br>password.) | Yes                    | Increment                                    |                  |
|                           | Yes                       | No                                                                 | Yes                    | Increment                                    |                  |
|                           | No                        | N/A                                                                | Yes                    | Increment                                    |                  |
|                           | No                        | N/A                                                                | No                     |                                              | Increment        |
| 1. Public Key<br>(only)   | Yes                       | Yes                                                                | N/A                    | Increment                                    |                  |
|                           | Yes                       | Yes (No match<br>between client<br>and server. Go<br>go password.) |                        |                                              | Increment        |
|                           | Yes                       |                                                                    | N/A                    |                                              | Increment        |
|                           | No                        |                                                                    | N/A                    |                                              | Increment        |

TABLE

```
*A:Dut-C# show system security user detail
=====
Users
=====
User ID New User Permissions Password Login Failed Local
 Pwd console ftp li snmp Expires Attempts Logins Conf

admin n y n n n never 4 0 y

Number of users : 1
```

```

=====
User Configuration Detail
=====
user id : admin

console parameters

new pw required : no cannot change pw : no
home directory :
restricted to home : no
login exec file :
profile : administrative

snmp parameters

=====

```

## 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 25: Show View Output Fields**

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

### Sample Output

```
A:ALA-48# show system security view
```

```
=====
Views
=====
view name oid tree mask permission

iso 1 11111111 included
read1 1.1.1.1 11111111 included
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 11111111 included
mgmt-view 1.3.6.1.2.1.4 11111111 included
mgmt-view 1.3.6.1.2.1.5 11111111 included
mgmt-view 1.3.6.1.2.1.6 11111111 included
mgmt-view 1.3.6.1.2.1.7 11111111 included
mgmt-view 1.3.6.1.2.1.31 11111111 included
mgmt-view 1.3.6.1.2.1.77 11111111 included
mgmt-view 1.3.6.1.4.1.6527.3.1.2.3.7 11111111 included
mgmt-view 1.3.6.1.4.1.6527.3.1.2.3.11 11111111 included
no-security 1 11111111 included
no-security 1.3.6.1.6.3 11111111 excluded
no-security 1.3.6.1.6.3.10.2.1 11111111 included
no-security 1.3.6.1.6.3.11.2.1 11111111 included
no-security 1.3.6.1.6.3.15.1.1 11111111 included
on-security 2 00000000 included

No. of Views: 20
=====
A:ALA-48#
```

## certificate

**Syntax** **certificate**

**Context** show

**Description** This command displays certificate information.

## ca-profile

**Syntax** **ca-profile**  
**ca-profile** *name* [**association**]

**Context** show>certificate

**Description** This command shows certificate-authority profile information.

**Parameters** *name* — Specifies the name of the Certificate Authority (CA) profile.  
**association** — Displays associated CA profiles.

## ocsp-cache

|                    |                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ocsp-cache</b> [ <i>entry-id</i> ]                                                                                                                                                                                                                                         |
| <b>Context</b>     | show>certificate                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command displays the current cached OCSP results. The output includes the following information:</p> <ul style="list-style-type: none"><li>• Certificate issuer</li><li>• Certificate serial number</li><li>• OCSP result</li><li>• Cache entry expire time</li></ul> |
| <b>Parameters</b>  | <i>entry-id</i> — Specifies the local cache entry identifier of the certificate that was validated by the OCSP responder.                                                                                                                                                     |

## statistics

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>statistics</b>                                  |
| <b>Context</b>     | show>certificate                                   |
| <b>Description</b> | This command shows certificate related statistics. |

---

# 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 26: 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

|                    |                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>statistics</b> [ <b>interface</b> <i>ip-int-name</i>   <i>ip-address</i> ]                                                                                                                                                                                                                                  |
| <b>Context</b>     | clear>router>authentication                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command clears authentication statistics.                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <i>ip-int-name</i> — 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<br><i>ip-address</i> — Clears the authentication statistics for the specified IP address. |

### ip-filter

|                    |                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-filter</b> [ <b>entry</b> <i>entry-id</i> ]                                                    |
| <b>Context</b>     | clear>cpm-filter                                                                                     |
| <b>Description</b> | This command clears IP filter statistics.                                                            |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Specifies a particular CPM IP filter entry.<br><b>Values</b> 1 — 2048 |

### ipv6-filter

|                    |                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipv6-filter</b> [ <b>entry</b> <i>entry-id</i> ]                                                  |
| <b>Context</b>     | clear>cpm-filter                                                                                     |
| <b>Description</b> | This command clears IPv6 filter statistics.                                                          |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Specifies a particular CPM IP filter entry.<br><b>Values</b> 1 — 2048 |

## mac-filter

|                    |                                                                             |
|--------------------|-----------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mac-filter</b> [ <b>entry</b> <i>entry-id</i> ]                          |
| <b>Context</b>     | clear>cpm-filter                                                            |
| <b>Description</b> | This command clears MAC filter statistics.                                  |
| <b>Parameters</b>  | <b>entry</b> <i>entry-id</i> — Specifies a particular CPM MAC filter entry. |
| <b>Values</b>      | 1 — 2048                                                                    |

---

## CPU Protection Commands

### cpu-protection

|                    |                                                                |
|--------------------|----------------------------------------------------------------|
| <b>Syntax</b>      | <b>cpu-protection</b>                                          |
| <b>Context</b>     | clear                                                          |
| <b>Description</b> | This command enables the context to clear CPU protection data. |

### excessive-sources

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>excessive-sources</b>                                                          |
| <b>Context</b>     | clear>cpu-protection                                                              |
| <b>Description</b> | This command clears the records of sources exceeding their per-source rate limit. |

### protocol-protection

|                    |                                                                                     |
|--------------------|-------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>protocol-protection</b>                                                          |
| <b>Context</b>     | clear>cpu-protection                                                                |
| <b>Description</b> | This command clears the interface counts of packets dropped by protocol protection. |

### violators

|                    |                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>violators [port][interface][sap]</b>                                                                                               |
| <b>Context</b>     | clear>cpu-protection                                                                                                                  |
| <b>Description</b> | This command clears the rate limit violator record.                                                                                   |
| <b>Parameters</b>  | <b>port</b> — Clears entries for ports.<br><b>interface</b> — Clears entries for interfaces.<br><b>sap</b> — Clears entries for SAPs. |

## cpm-queue

|                    |                                               |
|--------------------|-----------------------------------------------|
| <b>Syntax</b>      | <b>cpm-queue</b> <i>queue-id</i>              |
| <b>Context</b>     | clear                                         |
| <b>Description</b> | This command clears CPM queue information.    |
| <b>Parameters</b>  | <i>queue-id</i> — Specifies the CPM queue ID. |
| <b>Values</b>      | 33 — 2000                                     |

## radius-proxy-server

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>radius-proxy-server</b> <i>server-name</i> <b>statistics</b>                                                          |
| <b>Context</b>     | clear>router                                                                                                             |
| <b>Description</b> | This command clears RADIUS proxy server data.                                                                            |
| <b>Parameters</b>  | <i>server-name</i> — Specifies the proxy server name.<br><b>statistics</b> — Clears statistics for the specified server. |

---

## Debug Commands

### radius

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

### ocsp

|                    |                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] ocsp</b>                                                                                                                       |
| <b>Context</b>     | debug                                                                                                                                  |
| <b>Description</b> | This command enables debug output of OCSP protocol for the CA profile.<br>The <b>no</b> form of the command disables the debug output. |

### ca-profile

|                    |                                                             |
|--------------------|-------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] ca-profile <i>profile-name</i></b>                  |
| <b>Context</b>     | debug>ocsp                                                  |
| <b>Description</b> | This command enables debug output of a specific CA profile. |

---

## Tools Commands

### dist-cpu-protection

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dist-cpu-protection</b>                                                                                                    |
| <b>Context</b>     | tools>perform>security<br>tools>dump>security                                                                                 |
| <b>Description</b> | This command displays to release Distributed CPU Protection parameters and status at the per card and forwarding plane level. |

### release-hold-down

|                    |                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>release-hold-down interface</b> <i>interface-name</i> [ <b>protocol</b> <i>protocol</i> ] [ <b>static-policer</b> <i>name</i> ]<br><b>release-hold-down sap</b> <i>sap-id</i> [ <b>protocol</b> <i>protocol</i> ] [ <b>static-policer</b> <i>name</i> ]                                                                       |
| <b>Context</b>     | tools>perform>security>dist-cput protection                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | This command is used to release a Distributed CPU Protection (DCP) policer from a hold-down countdown (or indefinite hold-down if configured as such).                                                                                                                                                                           |
| <b>Parameters</b>  | <b>interface</b> <i>interface-name</i> — Specifies Router interface name.<br><b>sap</b> <i>sap-id</i> — Specify sap identifier.<br><b>protocol</b> <i>protocol</i> — Specifies DCP protocol name (for example, arp, dhcp)<br><b>static-policer</b> <i>name</i> — Specifies DCP static policer name as defined in the DCP policy. |

### violators

|                    |                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>violators enforcement {sap interface} card</b> <i>slot-number</i> [ <b>fp</b> <i>fp-number</i> ]<br><b>violators local-monitor {sap interface} card</b> <i>slot-number</i> [ <b>fp</b> <i>fp-number</i> ]                                                                                                                                               |
| <b>Context</b>     | tools>dump>security>dist-cput protection                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | This command shows the non-conformant enforcement policers and local monitors.                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <b>sap</b> — -Indicates to display the violators associated with SAPs<br><b>interface</b> — - Indicates to display the violators associated with router interfaces.<br><b>enforcement</b> — Shows exceed and hold-down for Static and Dynamic Policers.<br><b>local-monitor</b> — Shows state of dynamic policer allocation for Local Monitoring Policers. |

**card** *slot-number* — The physical slot number for the card.

**Values** 1— n (n is platform dependant)

**fp** *fp-number* — Identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, an IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMAs).

**Values** 1— 2

**Output** **Users Output** — The following table describes show users output fields.

**Table 27: Output Parameters**

| Label            | Description                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Interface        | The name of the router interface                                                                                                         |
| Policer/Protocol | The configured name of the static policer (indicated with an [S]) or the DCP protocol name for a dynamic policer (indicated with a [D]). |
| [S] / [D]        | indicates a static vs dynamic policer                                                                                                    |
| Hld Rem          | The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.                               |

### Sample Output

```
*A:Dut-A# tools dump security dist-cpu-protection violators enforcement interface
card 4 fp 1
=====
Distributed Cpu Protection Current Interface Enforcer Policer Violators
=====
Interface Policer/Protocol Hld Rem

Violators on Slot-4 Fp-1

test staticArpPolicer [S] none
test icmp [D] none
test ospf [D] none

[S]-Static [D]-Dynamic [M]-Monitor
=====
```

---

## Admin Commands

### clear logout

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>clear logout</b> { <b>user</b> <i>name</i>   <b>all</b> }                      |
| <b>Context</b>     | admin>user                                                                        |
| <b>Description</b> | This command is used to clear any lockouts for a specific user, or for all users. |
| <b>Parameters</b>  | <i>name</i> — Specifies locked username.                                          |

### clear password-history

|                    |                                                                                        |
|--------------------|----------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>clear password-history</b> { <b>user</b> <i>name</i>   <b>all</b> }                 |
| <b>Context</b>     | admin>user                                                                             |
| <b>Description</b> | This command is used to clear old passwords used by a specific user, or for all users. |
| <b>Parameters</b>  | <i>name</i> — Specifies username.                                                      |



---

## In This Chapter

This chapter provides information to configure SNMP.

Topics in this chapter include:

- [SNMP Overview on page 282](#)
  - [SNMP Architecture on page 282](#)
  - [Management Information Base on page 282](#)
  - [SNMP Protocol Operations on page 283](#)
  - [SNMP Versions on page 283](#)
  - [Management Information Access Control on page 284](#)
  - [User-Based Security Model Community Strings on page 285](#)
  - [Views on page 285](#)
  - [Access Groups on page 285](#)
  - [Users on page 287](#)
  - [Per-VPRN Logs and SNMP Access on page 287](#)
  - [Per-SNMP Community Source IP Address Validation on page 287](#)
- [Which SNMP Version to Use? on page 288](#)
- [Configuration Notes on page 290](#)

## SNMP Overview

---

### SNMP Architecture

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

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

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

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

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

### Management Information Base

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

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

---

## SNMP Protocol Operations

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

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

## SNMP Versions

The agent supports multiple versions of the SNMP protocol.

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.  
SNMPv1 uses a community string match for authentication.
- The 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 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 router.

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

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

## User-Based Security Model Community Strings

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

---

## Views

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

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

The following system-provisioned views are available through the **config>system>security>snmp# view** context, which are particularly useful when configuring SNMPv1 and SNMPv2c:

- “iso” view—intended for administrative-type access to the entire supported object tree (except Lawful Interception)
- “no-security” view—similar to “iso” view, but removes access to several security areas of the object tree (such as SNMP communities, user and profile configuration, SNMP engine ID, etc). The “no-security” view is generally recommended over the “iso” view to reduce access to security objects.
- “li-view” view—provides access to a small set of Lawful Interception related objects
- “mgmt-view” view—provides access to IF-MIB and a few other basics
- “vprn-view” view—used to limit access to objects associated with a specific VPRN (for example, the Per-VPRN Logs and SNMP Access feature)

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.

When configuring access groups, the “no-security” view is generally recommended over the “iso” view in order to restrict access to security objects.

A set of system-provisioned access groups and system-created communities are available in SR OS. The system-provisioned groups and communities that begin with “cli-” are only used for internal CLI management purposes and are not exposed to external SNMP access.

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 router 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](#)).

## Per-VRN Logs and SNMP Access

Configuration of VRN-specific logs (with VRN-specific syslog destinations, SNMP trap/notification groups, etc) is supported in addition to the global logs configured under "config log". The event streams for vprn logs contain only events that are associated with the particular vprn.

Each VRN service can be configured with a set of SNMP v1/v2c community strings. These communities are mapped to the default "snmp-vprn" and "snmp-vprn-ro" views, which limit SNMP access to objects associated with a specific VRN. For example, walking the ifTable (IF-MIB) using the community configured for VRN 5 will return counters and status for VRN 5. See the "vprn <x> snmp community" command description for more details.

## Per-SNMP Community Source IP Address Validation

SNMPv1 and SNMPv2c requests can be validated against per-snmp-community whitelists (**src-access-list**) of configured source IPv4 and IPv6 addresses. Source IP address lists can be configured and then associated with an SNMP community.

SNMPv1 and SNMPv2c requests that fail the source IP address and community validation checks are discarded and are logged as SNMP event 2003 authenticationFailure (suppressed by default under "event-control").

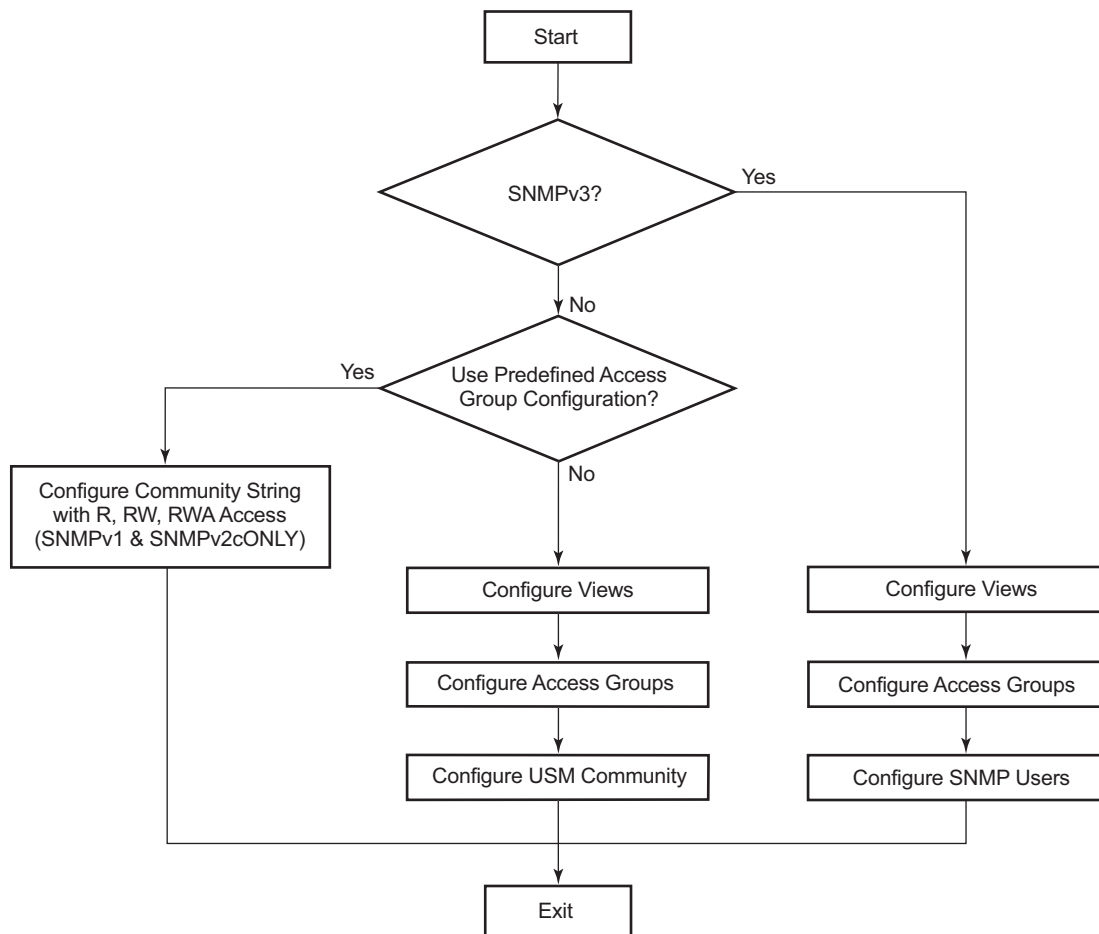
## Which SNMP Version to Use?

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 router. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

[Figure 7](#) depicts the configuration requirements to implement SNMPv1/SNMPv2c, and SNMPv3.





al\_0203

**Figure 7: 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 292](#)
- [Basic SNMP Security Configuration on page 293](#)
- [Configuring SNMP Components on page 294](#)

## SNMP Configuration Overview

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

- [Configuring SNMPv1 and SNMPv2c on page 292](#)
  - [Configuring SNMPv3 on page 292](#)
- 

## Configuring SNMPv1 and SNMPv2c

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

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

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

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

---

## Configuring SNMPv3

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

## Configuring SNMP Components

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

- [Configuring a Community String on page 295](#)
  - [Configuring View Options on page 295](#)
  - [Configuring Access Options on page 296](#)
  - [Configuring USM Community Options on page 297](#)
  - [Configuring Other SNMP Parameters on page 298](#)
- 

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

## Configuring a Community String

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

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

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

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

Use the following CLI syntax to configure community options:

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

The following displays an SNMP community configuration example:

```
*A:cses-A13>config>system>security>snmp# info

community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both

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

## Configuring View Options

Use the following CLI syntax to configure view options:

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

The following displays a view configuration example:

```
*A:cses-A13>config>system>security>snmp# info

view "testview" subtree "1"
mask ff
exit
view "testview" subtree "1.3.6.1.2"
mask ff type excluded
exit
```

```
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both

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

## Configuring Access Options

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

Use the following CLI syntax to configure access features:

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

The following displays an access configuration with the view configurations.

```
*A:cses-A13>config>system>security>snmp# info

view "testview" subtree "1"
mask ff
exit
view "testview" subtree "1.3.6.1.2"
mask ff type excluded
exit
access group "test" security-model usm security-level auth-no-pr
ivacy read "testview" write "testview" notify "testview"
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both

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

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

**CLI Syntax:** config>system>security# user user-name  
 access [ftp] [snmp] [console]  
 snmp  
 authentication [none] | [[hash] {md5 key|sha key } privacy  
 {none|des-key|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 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 "L1a.RtAyRW2" hash2 r version v2c
 community "r0a159kIOfg" hash2 r version both

A:ALA-1>config>system>security>snmp#
```

The group **group**test 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
 — streaming
 — [no] shutdown
 — [no] shutdown

```

#### SNMP Security Commands

Refer to the 7x50 SR OS Services Guide for information about configuring SNMP in a VPRN service.

```

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

```

## Command Hierarchies

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
 — streaming
 — counters
 — system
 — information
 — security
 — access-group [group-name]
 — authentication [statistics]
 — password-options [entry-id]
 — password-options
 — per-peer-queuing
 — profile [profile-name]
 — snmp
 — community [community-string]
 — src-access-list [list-name]
 — ssh
 — user [user-id] [detail]
 — view [view-name] [detail]
```

---

## Configuration Commands

---

### SNMP System Commands

---

#### engineID

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

#### general-port

|                    |                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>general-port</b> <i>port-number</i><br><b>no general-port</b>                                                                                                                                                                                                                |
| <b>Context</b>     | config>system>snmp                                                                                                                                                                                                                                                              |
| <b>Description</b> | 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 <b>config&gt;log&gt;snmp-trap-group&gt;trap-target</b> 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.

### streaming

**Syntax** **snmp**

**Context** config>system>snmp>streaming

**Description** This command enables the proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes. In higher latency networks, synchronizing router MIBs from network management via streaming takes less time than synchronizing via classic SNMP UDP requests. Streaming operates on TCP port 1491 and runs over IPv4 or IPv6.

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>system>snmp>streaming                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command administratively disables proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes..</p> <p>The <b>no</b> form of the command administratively re-enables SNMP request/response bundling and TCP-based transport mechanism.</p> |
| <b>Default</b>     | <b>shutdown</b>                                                                                                                                                                                                                                                                                                           |

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>system>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>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 <b>config&gt;log&gt;snmp-trap-group</b> context.</p> <p>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 <b>bof persist on</b> command is enabled.</p> <p>The <b>no</b> form of the command administratively enables SNMP which is the default state.</p> |
| <b>Default</b>     | <b>no shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

## SNMP Security Commands

### access group

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] access group</b> <i>group-name</i> <b>security-model</b> <i>security-model</i> <b>security-level</b> <i>security-level</i> [ <b>context</b> <i>context-name</i> [ <b>prefix-match</b> ]] [ <b>read</b> <i>view-name-1</i> ] [ <b>write</b> <i>view-name-2</i> ] [ <b>notify</b> <i>view-name-3</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>system>security>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <p>This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.</p> <p>Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the <b>community</b> on page 306).</p> <p>Default access group configurations cannot be modified or deleted.</p> <p>To remove the user group with associated, security model(s), and security level(s), use:<br/> <b>no access group</b> <i>group-name</i></p> <p>To remove a security model and security level combination from a group, use:<br/> <b>no access group</b> <i>group-name</i> <b>security-model</b> {snmpv1   snmpv2c   usm} <b>security-level</b> {no-auth-no-privacy   auth-no-privacy   privacy}</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><i>group-name</i> — Specify a unique group name up to 32 characters.</p> <p><b>security-model</b> {snmpv1   snmpv2c   usm} — Specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.</p> <p><b>security-level</b> {no-auth-no-priv   auth-no-priv   privacy} — Specifies the required authentication and privacy levels to access the views configured in this node.</p> <p><b>security-level no-auth-no-privacy</b> — Specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the <b>none</b> option.</p> <p><b>security-level auth-no-privacy</b> — Specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the <b>group</b> and the <b>user</b> must be configured for authentication.</p> <p><b>security-level privacy</b> — Specifies that both authentication and privacy (encryption) is required. When this option is configured, both the <b>group</b> and the user must be configured for <b>authentication</b>. The user must also be configured for <b>privacy</b>.</p> <p><b>context</b> <i>context-name</i> — Specifies a set of SNMP objects that are associated with the context-name.</p> |



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

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

**Default** none

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

**Values** Up to 32 characters

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

**Values** none

## attempts

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

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

**Default** 10

**Values** 0 — 1440

## community

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>community</b> <i>community-string</i> [ <b>hash</b>   <b>hash2</b> ] <i>access-permissions</i> [ <b>version</b> <i>SNMP-version</i> ]<br><b>[src-access-list</b> <i>list-name</i> ]<br><b>no community</b> <i>community-string</i> [ <b>hash</b>   <b>hash2</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>system>security>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | <p>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 <b>usm-community</b> command.</p> <p>When configured, community implies a security model for SNMPv1 and SNMPv2c only. For SNMPv3 security, the <b>access group</b> command on page 304 must be configured.</p> <p>The <b>no</b> form of the command removes a community string.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <p><i>community-string</i> — Configure the SNMPv1 and/or SNMPv2c community string.</p> <p><b>Values</b></p> <ul style="list-style-type: none"> <li><i>community-string</i> — 32 characters maximum</li> <li><i>hash-key</i> — 33 characters maximum</li> <li><i>hash2-key</i> — 96 characters maximum</li> </ul> <p><b>hash</b>   <b>hash2</b> — Configures the hashing scheme for <i>community-string</i>. <b>Hash</b> specifies that the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form. <b>Hash2</b> specifies that the key is entered in a more complex encrypted form.</p> <p><i>access-permissions</i> — •Configures the access permissions for objects in the MIB.</p> <ul style="list-style-type: none"> <li>• <b>r</b> — Grants only read access to objects in the MIB, except security objects.</li> <li>• <b>rw</b> — Grants read and write access to all objects in the MIB, except security.</li> <li>• <b>rwa</b> — Grants read and write access to all objects in the MIB, including security.</li> <li>• <b>vpls-mgmt</b> — Assigns a unique SNMP community string to the management virtual router.</li> </ul> <p><b>version</b> {<b>v1</b>   <b>v2c</b>   <b>both</b>} — Configures the scope of the community string to be for SNMPv1, SNMPv2c, or both SNMPv1 and SNMPv2c access.</p> <p><b>Default</b> <b>both</b></p> |

*list-name* — Configures the **community** to reference a specific **src-access-list**, which will be used to validate the source IP address of all received SNMP requests that use this **community**. Multiple **community** instances can reference the same **src-access-list**. 32 characters maximum.

## mask

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mask</b> <i>mask-value</i> [ <b>type</b> { <b>included</b>   <b>excluded</b> } ]<br><b>no mask</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>system>security>snmp>view <i>view-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>The mask value and the mask type, along with the <i>oid-value</i> configured in the <b>view</b> command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Per RFC 2575, <i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>, 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 <i>vacmViewTreeFamilyType</i> in the entry whose value of <i>vacmViewTreeFamilySubtree</i> has the most sub-identifiers.</p> <p>The <b>no</b> form of this command removes the mask from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <p><i>mask-value</i> — The mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view. (Default: all 1<sup>s</sup>)</p> <p>The mask can be entered either:</p> <ul style="list-style-type: none"> <li>• In hex. For example, 0xfc.</li> <li>• In binary. For example, 0b11111100.</li> </ul> <p>Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.</p> <p><b>type {included   excluded}</b> — Specifies whether to include or exclude MIB subtree objects. <i>included</i> - All MIB subtree objects that are identified with a 1 in the mask are available in the view. (Default: <i>included</i>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

*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

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

### src-access-list

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-access-list</b> <i>list-name</i><br><b>no src-access-list</b> <i>list-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>system>security>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>This command is used to identify a list of source IP addresses that can be used to validate SNMPv1 and SNMPv2c requests once the list is associated with one or more SNMPv1 and SNMPv2c communities.</p> <p>An <b>src-address-list</b> referenced by one or more <b>community</b> instances is used to verify the source IP addresses of an SNMP request using the <b>community</b> regardless of which VPRN/VRF interface (or 'Base' interface) the request arrived on. For example, if an SNMP request arrives on an interface in vprn 100 but the request is referencing a <b>community</b>, then the source IP address in the packet would be validated against the <b>src-address-list</b> configured for the <b>community</b>. This occurs regardless of whether the request is destined to a VPRN interface address and the VPRN has SNMP access enabled, or the request is destined to the base system address via GRT leaking. If the request's source IP address does not match the <i>ip-address</i> of any of the <b>src-hosts</b> contained in the list, then the request will be discarded and logged as an SNMP authentication failure.</p> <p>Using <b>src-access-list</b> validation can have an impact on the time it takes for an SR OS node to reply to an SNMP request. It is recommended to keep the lists short, including only the addresses that are needed, and to place SNMP managers that send the highest volume of requests, such as the 5620 SAM, at the top of the list.</p> <p>You can configure a maximum of 16 <b>src-access-lists</b>. Each <b>src-access-list</b> can contain a maximum of 16 <b>src-hosts</b>.</p> <p>The <b>no</b> form of this command removes the named <b>src-access-list</b>. You cannot remove an <b>src-access-list</b> that is referenced by one or more <b>community</b> instances.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <i>list-name</i> — Configures the name or key of the <b>src-access-list</b> . The <i>list-name</i> parameter must begin with a letter (a-z or A-Z).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## src-host

|                    |                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                     |              |         |  |              |                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------|---------|--|--------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-host</b> <i>host-name</i> <b>address</b> <i>ip-address</i><br><b>no src-host</b> <i>host-name</i>                                                                                                                                                                                                                                                                                                      |                                                                     |              |         |  |              |                                                                     |
| <b>Context</b>     | config>system>security>snmp>src-access-list                                                                                                                                                                                                                                                                                                                                                                   |                                                                     |              |         |  |              |                                                                     |
| <b>Description</b> | <p>This command is used to configure a source IP address entry that can be used to validate SNMPv1 and SNMPv2c requests.</p> <p>The <b>no</b> form of this command removes the specified entry.</p>                                                                                                                                                                                                           |                                                                     |              |         |  |              |                                                                     |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                     |              |         |  |              |                                                                     |
| <b>Parameters</b>  | <p><i>host-name</i> — Configures the name of the <b>src-host</b> entry.</p> <p><i>ip-address</i> — Configures an allowed source address for SNMP requests. This can be an IPv4 or IPv6 address.</p> <table><tr><td><b>Values</b></td><td>ipv4-address</td><td>a.b.c.d</td></tr><tr><td></td><td>ipv6-address</td><td>x:x:x:x:x:x:x<br/>x:x:x:x:x:d.d.d.d<br/>x: [0..FFFF]H<br/>d: [0..255]D</td></tr></table> | <b>Values</b>                                                       | ipv4-address | a.b.c.d |  | ipv6-address | x:x:x:x:x:x:x<br>x:x:x:x:x:d.d.d.d<br>x: [0..FFFF]H<br>d: [0..255]D |
| <b>Values</b>      | ipv4-address                                                                                                                                                                                                                                                                                                                                                                                                  | a.b.c.d                                                             |              |         |  |              |                                                                     |
|                    | ipv6-address                                                                                                                                                                                                                                                                                                                                                                                                  | x:x:x:x:x:x:x<br>x:x:x:x:x:d.d.d.d<br>x: [0..FFFF]H<br>d: [0..255]D |              |         |  |              |                                                                     |

## usm-community

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>usm-community</b> <i>community-string</i> <b>group</b> <i>group-name</i><br><b>no usm-community</b> <i>community-string</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>system>security>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | 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.<br><br>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.<br><br>The <b>no</b> form of this command removes a community string. |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>community-string</i> — Configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used.<br><br><i>group</i> — Specify the group that governs the access rights of this community string. This group must be configured first in the <b>config system security snmp access group</b> context.<br>(Default: none)                                                                                                                                                                                                                                                                                                                                                |

## view

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>view</b> <i>view-name</i> <b>subtree</b> <i>oid-value</i><br><b>no view</b> <i>view-name</i> [ <b>subtree</b> <i>oid-value</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>system>security>snmp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.</p> <p>Once the subtree (OID) is identified, a mask can be created to select the portions of the subtree to be included or excluded for access using this particular view. See the <b>mask</b> command. The view(s) configured with this command can subsequently be used in read, write, and notify commands which are used to assign specific access group permissions to created views and assigned to particular access groups.</p> <p>Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.</p> <p>The <b>no view</b> <i>view-name</i> command removes a view and all subtrees.</p> <p>The <b>no view</b> <i>view-name</i> <b>subtree</b> <i>oid-value</i> removes a sub-tree from the view name.</p> |
| <b>Default</b>     | No views are defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><i>view-name</i> — Enter a 1 to 32 character view name. (Default: <i>none</i>)</p> <p><i>oid-value</i> — The object identifier (OID) value for the <i>view-name</i>. 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.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Show Commands

### counters

|                    |                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>counters</b>                                                                                                                                                             |
| <b>Context</b>     | show>snmp                                                                                                                                                                   |
| <b>Description</b> | 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. |
| <b>Output</b>      | <b>Counters Output</b> — The following table describes SNMP counters output fields.                                                                                         |

**Table 28: 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#

```

## counters

- Syntax** **counters**
- Context** show>snmp>streaming
- Description** This command displays counters information for the proprietary SNMP streaming protocol. Output: Counters Output - The following table describes SNMP streaming counters output fields.
- Output** **Counters Output** — The following table describes SNMP streaming counters output fields.

**Table 29: Counters Output Fields**

| Label         | Description                                               |
|---------------|-----------------------------------------------------------|
| in getTables  | Displays the number of GetTable request packets received. |
| in getManys   | Displays the number of GetMany request packets received.  |
| out responses | Displays the number of response packets sent.             |

### Sample Output

```

*A:Dut-B# show snmp streaming counters
=====
STREAMING counters:
=====
 in getTables : 772
 in getManys : 26

 out responses : 848
=====

```



## information

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

**Table 30: 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.<br>Disabled — SNMP is administratively disabled.                                                                                  |
| SNMP Oper State        | Enabled — SNMP is operationally enabled.<br>Disabled — SNMP is operationally disabled.                                                                                        |
| SNMP Index Boot Status | Persistent — Persistent indexes at the last system reboot was enabled.<br>Disabled — Persistent indexes at the last system reboot was disabled.                               |
| SNMP Sync State        | The state when the synchronization of configuration files between the primary and secondary s finish.                                                                         |
| Telnet/SSH/FTP Admin   | Displays the administrative state of the Telnet, SSH, and FTP sessions.                                                                                                       |

**Table 30: Show System Information Output Fields (Continued)**

| Label                   | Description                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet/SSH/FTP Oper     | Displays the operational state of the Telnet, SSH, and FTP sessions.                                                                                                                                                                                                                                                                                                                         |
| BOF Source              | The boot location of the BOF.                                                                                                                                                                                                                                                                                                                                                                |
| Image Source            | <p><code>primary</code> — Specifies whether the image was loaded from the primary location specified in the BOF.</p> <p><code>secondary</code> — Specifies whether the image was loaded from the secondary location specified in the BOF.</p> <p><code>tertiary</code> — Specifies whether the image was loaded from the tertiary location specified in the BOF.</p>                         |
| Config Source           | <p><code>primary</code> — Specifies whether the configuration was loaded from the primary location specified in the BOF.</p> <p><code>secondary</code> — Specifies whether the configuration was loaded from the secondary location specified in the BOF.</p> <p><code>tertiary</code> — Specifies whether the configuration was loaded from the tertiary location specified in the BOF.</p> |
| Last Booted Config File | Displays the URL and filename of the configuration file used for the most recent boot.                                                                                                                                                                                                                                                                                                       |
| Last Boot Cfg Version   | Displays the version of the configuration file used for the most recent boot.                                                                                                                                                                                                                                                                                                                |
| Last Boot Config Header | Displays header information of the configuration file used for the most recent boot.                                                                                                                                                                                                                                                                                                         |
| Last Boot Index Version | Displays the index version used in the most recent boot.                                                                                                                                                                                                                                                                                                                                     |
| Last Boot Index Header  | Displays the header information of the index used in the most recent boot.                                                                                                                                                                                                                                                                                                                   |
| Last Saved Config       | Displays the filename of the last saved configuration.                                                                                                                                                                                                                                                                                                                                       |
| Time Last Saved         | Displays the time the configuration was most recently saved.                                                                                                                                                                                                                                                                                                                                 |
| Changes Since Last Save | <p><code>Yes</code> — The configuration changed since the last save.</p> <p><code>No</code> — The configuration has not changed since the last save.</p>                                                                                                                                                                                                                                     |
| 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.                                                                                                                                                                                                                                  |

**Table 30: Show System Information Output Fields (Continued)**

| <b>Label</b>           | <b>Description</b>                                                                                                                                                                                                                                |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cfg-OK Script          | URL — The location and name of the CLI script file executed following successful completion of the boot-up configuration file execution.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Next Hop — The next hop IP address used to reach the destination.<br><br>Metric — Displays the priority of this static route versus other static routes.<br><br>None — No static routes are configured. |

## Sample Output

A:ALA-1# show system information

### System Information

```
=====
System Name : ALA-1
System Type : 7450 ESS-7
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 7450
 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 7450
 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 :
```

## 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 31: 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 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 iso
snmp-trap snmpv2c none iso iso

No. of Access Groups: 8
=====
A:ALA-1#

A:ALA-1# show system security access-group detail
```

```

=====
Access Groups
=====
group name security security read write notify
 model level view view view

snmp-ro snmpv1 none no-security no-security

No. of Access Groups:
...
=====
A:ALA-1#

```

## authentication

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

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

| Label          | Description (Continued)                                                                                                                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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#
```

## password-options

|                    |                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>password-options</b>                                                                        |
| <b>Context</b>     | show>system>security                                                                           |
| <b>Description</b> | This command displays password options.                                                        |
| <b>Output</b>      | <b>Password-Options Output</b> — 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.                       |

| Label                                          | Description                                                                                                                                                    |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lockout period<br>(when threshold<br>breached) | Displays the number of minutes the user is locked out if the threshold of unsuccessful login attempts has exceeded.                                            |
| Authentication<br>order                        | Displays the most preferred method to authenticate and authorize a user.                                                                                       |
| Configured com-<br>plexity options             | Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the <b>authentication</b> section. |
| Minimum password<br>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

|                    |                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>per-peer-queuing</b>                                                                                                      |
| <b>Context</b>     | show>system>security                                                                                                         |
| <b>Description</b> | 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\_Queueing Output** — The following table describes the per-peer-queueing output fields.

| Label                | Description                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Per Peer Queueing    | Displays whether per-peer-queueing 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 queueing 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-queueing
=====
CPM Hardware Queueing
=====
Per Peer Queueing : Enabled
Total Num of Queues : 8192
Num of Queues In Use : 0
=====
A:ALA-48>show>system>security#
```

## profile

|                    |                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>profile</b> [ <i>profile-name</i> ]                                                                                                                                           |
| <b>Context</b>     | show>system>security                                                                                                                                                             |
| <b>Description</b> | This command displays user profiles for CLI command tree permissions.                                                                                                            |
| <b>Parameters</b>  | <i>profile-name</i> — 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. |
| <b>Output</b>      | <b>Profile Output</b> — 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.<br><br>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.<br><br>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 | <p><b>administrative</b> — Enables the user to execute all commands.</p> <p><b>configure system security</b> — Enables the user to execute the <b>config system security</b> command.</p> <p><b>enable-admin</b> — Enables the user to enter a special administrative mode by entering the <b>enable-admin</b> command.</p> <p><b>exec</b> — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console.</p> <p><b>exit</b> — Enables the user to execute the <b>exit</b> command.</p> <p><b>help</b> — Enables the user to execute the <b>help</b> command.</p> <p><b>logout</b> — Enables the user to execute the <b>logout</b> command.</p> <p><b>password</b> — Enables the user to execute the <b>password</b> command.</p> <p><b>show config</b> — Enables the user to execute the <b>show config</b> command.</p> <p><b>show</b> — Enables the user to execute the <b>show</b> command.</p> <p><b>show system security</b> — Enables the user to execute the <b>show system security</b> command.</p> |
| Action        | <p><b>permit</b> — Enables the user access to all commands.</p> <p><b>deny-all</b> — Denies the user access to all commands.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

```

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#

```

## snmp

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Syntax</b>      | <b>snmp</b>                                                |
| <b>Context</b>     | show>system>security                                       |
| <b>Description</b> | This command enables the context to show SNMP information. |

## community

|                    |                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>community</b> [ <i>community-string</i> ]                                                                                                                                                                                                         |
| <b>Context</b>     | show>system>security>snmp                                                                                                                                                                                                                            |
| <b>Description</b> | This command lists SNMP communities and characteristics. Including the <i>community-name</i> parameter modifies the output to include all details for the specified community, including the source IP address list and validation failure counters. |
| <b>Output</b>      | <b>Community Output</b> — The following table describes the community output fields.                                                                                                                                                                 |

## Sample Output

Table 32: Show Community Output Fields

| Label             | Description                                                                                                                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Community         | The community string name for SNMPv1 and SNMPv2c access only.                                                                                                                                                                                  |
| Access            | r — The community string allows read-only access.<br>rw — The community string allows read-write access.<br>rwa — The community string allows read-write access.<br>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.                                                                                                                                                                                                                         |
| src-access-list   | The name of the list of source IP addresses that are allowed to use the community, as configured using the <b>community</b> configuration command.                                                                                             |
| authFailures      | The number of SNMP requests that have failed validation using this <b>community</b> .                                                                                                                                                          |
| No of Communities | The total number of configured community strings.                                                                                                                                                                                              |

**Note:** The system-created communities that begin with “cli-” are only used for internal CLI management purposes and are not exposed to external SNMP access.

```
A:ALA-1# show system security snmp community
```

```
=====
Communities
=====
community access view version group name

cli-li-readwrite n/a li-view v2c cli-li-readwrite
cli-readonly r iso v2c cli-readonly
cli-readwrite rw iso v2c cli-readwrite
my-private1 rw iso v1 v2c snmp-rwa
my-public2 r no-security v1 v2c snmp-ro
test-123 rwa n/a v2c snmp-trap

No. of Communities: 6
=====
A:ALA-1#
```

```
A:ALA-1# show system security snmp community "my-public2"
```

```
=====
```

```

Communities
=====
community access view version group name
 src-access-list authFailures

my-public2 r no-security v1 v2c snmp-ro
 my-list1 5
=====
A:ALA-1#

```

## src-access-list

- Syntax** **src-access-list** [*list-name*]
- Context** show>system>security>snmp
- Description** This command displays source access lists and the hosts for each. Including the *list-name* parameter modifies the output show only the specified **src-access-list**.
- Output** **Source Access List Output** — The following table describes the source access list output fields.

### Sample Output

**Table 33: Show Source Access List Output Fields**

| Label              | Description                                        |
|--------------------|----------------------------------------------------|
| List Name          | The name of the <b>src-access-list</b> .           |
| Host Name          | The name of the <b>src-host</b> .                  |
| Host Address       | The IP address of the <b>src-host</b> .            |
| Total Access Lists | The total number of source access lists displayed. |

```

A:ALA-1# show system security snmp src-access-list
=====
Source Access Lists
=====
List Name
 HostName Host Address

L1
 H1 100.100.100.1
 H2 100.100.100.2
L2
 HA 100.100.101.1
 HB 100.100.101.2

Total Access Lists: 2
=====
A:ALA-1#

```

```

A:ALA-1# show system security snmp src-access-list L1
=====
Source Access Lists
=====
List Name
 HostName Host Address

L1
 H1 100.100.100.1
 H2 100.100.100.2

Total Access Lists: 1
=====
A:ALA-1#

```

## 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 34: Show SSH Output Fields**

| Label                  | Description                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH status             | SSH is enabled — Displays that SSH server is enabled.<br><br>SSH is disabled — Displays that SSH server is disabled.                                                                                                                               |
| Key fingerprint        | The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed. |
| Connection             | The IP address of the connected router(s) (remote client).                                                                                                                                                                                         |
| Encryption             | des — Data encryption using a private (secret) key.<br><br>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 35: Show User Output Fields**

| Label            | Description                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User ID          | The name of a system user.                                                                                                                                                                           |
| Need New PWD     | Yes — The user must change his password at the next login.<br>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.<br>FTP — Specifies whether the user is permitted FTP access.<br>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.<br>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
```

## 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 36: Show System Security View Output Fields**

| Label        | Description                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View name    | The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.                                                                                        |
| OID tree     | The Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.                                                                                                                    |
| Mask         | The mask value and the mask type, along with the <i>oid-value</i> configured in the <b>view</b> 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.<br>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#

```



---

## In This Chapter

This chapter provides information to configure NETCONF.

Topics in this chapter include:

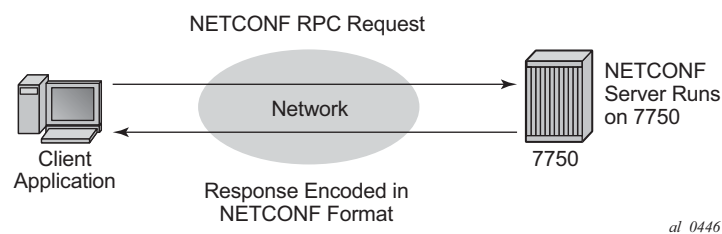
- [NETCONF Overview](#)
  - [NETCONF Introduction on page 334](#)
  - [NETCONF in SR OS on page 335](#)
  - [Establishing a NETCONF Session on page 351](#)
  - [XML Content Layer on page 352](#)
  - [XML Content Layer Examples on page 359](#)
  - [CLI Content Layer on page 362](#)
  - [CLI Content Layer Examples on page 363](#)

## NETCONF Overview

---

### NETCONF Introduction

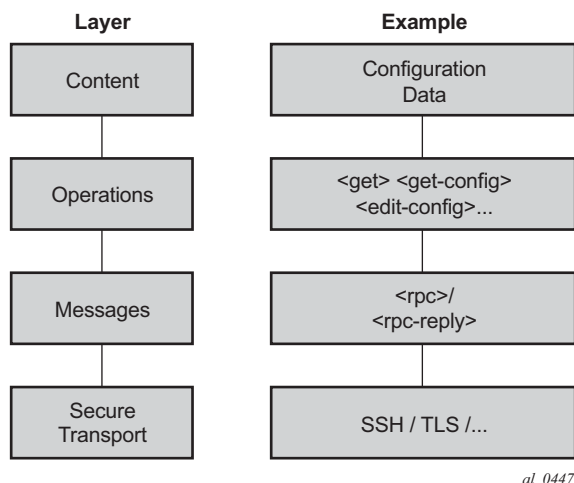
NETCONF is a standardized IETF configuration management protocol published in RFC 6241. It is secure, connection oriented, and runs on top of the SSHv2 transport protocol as specified in RFC 6242. NETCONF can be used as an alternative to CLI or SNMP for managing an SR OS node.



**Figure 8: NETCONF RPC Request**

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

NETCONF can be conceptually partitioned into four layers as described in RFC 6241.



**Figure 9: NETCONF Layers (RFC 6241)**

## NETCONF in SR OS

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

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

NETCONF is not used for notifications; for example, log events, syslog, or SNMP notifications (traps).

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

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

"bof", "debug", "tools", and other general CLI operational commands (e.g. "telnet" or "ping") are not supported via NETCONF.

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

SR OS supports both a CLI content layer and an XML-based content layer for NETCONF.

## YANG Data Models

The SR OS NETCONF XML content layer configuration schema is described in a set of Alcatel-Lucent proprietary YANG modules. The configuration modules are advertised in the SR OS NETCONF server hello.

The configuration YANG data model closely aligns to the SR OS CLI configuration tree structure and commands.

A set of YANG modules are published and distributed as part of an SR OS image in the cflash/support directory (along with files like dictionary-freeradius.txt and stats.dtd).

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

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

## Transport and Sessions

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

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

A client establishing a NETCONF session must log into the router so user accounts must exist for NETCONF on the SR. A new access type 'netconf' is provided. The user must be configured with both 'console' and 'netconf' access.

Only authentication via the local user database is supported for NETCONF users/sessions (no RADIUS or TACACS+ authentication). Access to various CLI config and show commands (authorization) via NETCONF is controlled through the profile assigned to the user that is used to authenticate the underlying SSH session.

Access to LI commands is based on the "access li" setting for the user.

If a NETCONF request attempts to execute a CLI command which is outside the scope of its access profile, an error response will be sent. For example:

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



```

 <get>
 <filter>
 <oper-data-format-cli-block>
 <cli-show>system security</cli-show>
 </oper-data-format-cli-block>
 </filter>
 </get>
 </rpc>
]]>]]>

```

Reply:

```

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

```

## NETCONF Operations

The following base protocol operations are supported:

- <get>
- <get-config>
- <edit-config>
- <copy-config>
- <delete-config>
- <validate>
- <close-session>
- <kill-session>

The <lock> and <unlock> base protocol operations are not supported.

The <error-option> is not supported. SR OS implements the stop-on-error behavior by default. The continue-on-error and rollback-on-error are not supported.

**<get>**

CLI content layer <get> operation is supported. XML content layer <get> operation is not supported.

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

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

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

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

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

Reply:

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

=====
Interface Table (Router: Base)
=====
Interface-Name Adm Opr (v4/v6) Mode Port/SapId
IP-Address PfxState

system Up Up/Down Network system
144.23.63.5/32 n/a

Interfaces : 1
=====
 </response>
```

```

 </item>
 <item>
 <cli-show>router mpls lsp</cli-show>
 <response>
 MINOR: CLI MPLS is not configured.
 </response>
 <rpc-error>
 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>cli-show</err-element>
 </error-info>
 <error-message>
 command failed - 'show router mpls lsp'
 </error-message>
 </rpc-error>
 </item>
 </oper-data-format-cli-block>
</data>
</rpc-reply>
]]>]]>

```

## <get-config>

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

## <edit-config>

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

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

## <copy-config> and <delete-config>

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

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

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

- `<source>=<running>` and `<target>=<startup>`
  - Ø Equivalent of "admin save"
  - Ø An index file is also saved if "persist on" is configured in the bof

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

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

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

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

- `<url>`
- `<startup>`

`<delete-config>` is not allowed on the `<running>` datastore.

## **`<validate>`**

The `validate:1.1` capability is supported:

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

## **Datastores and URLs**

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

All configuration changes (`<edit-config>`) done to the `<running>` datastore via NETCONF take immediate operational effect.

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

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

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

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

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

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

The following examples show the format of each URL scheme (Note the “///” for the ‘file’ URL. The ‘file://localhost/...’ format is not supported.):

- <target><url>ftp://name:passwd@a.b.c.d/usr/fredf/myfile.cfg</url></target>
- <target><url>tftp://name:passwd@a.b.c.d/usr/fredf/myfile.cfg</url></target>
- <target><url>file:///cf3:/myfiles/myfile.cfg</url></target>
- **Note:** The following format is also supported (no 'file:///'): <target><url>cf3:/myfiles/myfile.cfg</url></target>

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

The bof is not considered as part of any config datastore.

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

Lawful Interception configuration information is contained in the <running> datastore but is not saved in the <startup> datastore. The equivalent of the CLI "li save" command is available in an <edit-config>.

Configuration changes done via NETCONF are subject to CLI Rollback (revert, save, etc) and are included in the configuration when the operator performs an "admin save" in CLI.

## General NETCONF behavior

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

In the rpc tag, the only allowable namespace or prefix declaration is for the standard NETCONF “urn:ietf:params:xml:ns:netconf:base:1.0” namespace. If any other namespace is

declared (or assigned to a prefix) in the rpc tag then the SR OS server will reply with an error. XML namespace or prefix declarations in the rest of the request are accepted but ignored and unused. The SR OS NETCONF server puts correct namespace declarations in all replies. The SR OS NETCONF implementation does not support XML namespaces (xmlns).

**Example 1** — The standard NETCONF namespace

“urn:ietf:params:xml:ns:netconf:base:1.0” defined more than once in the rpc tag:

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

Reply (no error message):

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data>
 <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
 <router>
 <router-name>Base</router-name>
 <interface>
 <interface-name>system</interface-name>
 <address>
 <ip-address-mask>144.23.63.5/32</ip-address-mask>
 </address>
 <shutdown>false</shutdown>
 </interface>
 </router>
 </configure>
 </data>
</rpc-reply>
]]>]]>
```

**Example 2** — A non-standard NETCONF namespace defined in the rpc tag:

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

```

<source> <running/> </source>
<filter>
 <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
 <router>
 <interface>
 <interface-name>"system"</interface-name>
 </interface>
 </router>
 </configure>
</filter>
</get-config>
</rpc>
]]>]]>

```

Reply (an error message: An unexpected namespace is present):

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
 <rpc-error>
 <error-type>protocol</error-type>
 <error-tag>unknown-element</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <bad-element></bad-element>
 <bad-namespace>urn:alcatel-lucent.com:sros:ns:yang:conf-r13</bad-namespace>
 </error-info>
 <error-message>
 An unexpected namespace is present.
 </error-message>
 </rpc-error>
</rpc-reply>

```

**Example 3** — A non-standard NETCONF namespace used in one of the tags but not defined in the rpc tag:

```

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

```

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

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data>
 <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
 <router>
 <router-name>Base</router-name>
 <interface>
 <interface-name>system</interface-name>
 <address>
 <ip-address-mask>144.23.63.5/32</ip-address-mask>
 </address>
 <shutdown>false</shutdown>
 </interface>
 </router>
 </configure>
 </data>
</rpc-reply>
]]>]]>

```

**Example 4** — A non-standard NETCONF namespace/prefix used in one of the tags but not defined in the rpc tag:

```

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

```

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

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns:alu="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data>
 <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
 <router>
 <router-name>Base</router-name>
 <interface>
 <interface-name>system</interface-name>
 <address>
 <ip-address-mask>144.23.63.5/32</ip-address-mask>
 </address>
 <shutdown>false</shutdown>
 </interface>
 </router>
 </configure>
 </data>
</rpc-reply>
]]>]]>

```



```

 </router>
 </configure>
 </data>
 </rpc-reply>
]]>]]>

```

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

#### Example 1 — Chunked message:

```

#302
<?xml version="1.0" encoding="UTF-8"?><rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><get-config><source><running/></
source><filter><config><configure><router><interface><interface-name>system</inter-
face-name></interface></router></configure></config></filter></get-config></rpc>
##

```

#### Example 2 — Chunked message:

```

#38
<?xml version="1.0" encoding="UTF-8"?>
#85
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <get-config>
#62
 <source><running/></source>
 <filter>
 <configure>
#79
 <system>
 <netconf>
 </netconf>
 </system>
#55
 </configure>
 </filter>
 </get-config>
 </rpc>
##

```

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

```

<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=trim</
capability>

```

Pseudo-transactional capabilities are supported. A user can save a rollback checkpoint (for example, prior to doing an <edit-config> or a series of <edit-config>) and perform a rollback revert if needed later.

**Example 1** — Two rollback items with responses:

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

**Reply:**

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="102" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
 <cli-action>
 <item>
 <admin>rollback compare active-cfg to 1</admin>
 <response>
0.150 s
0.450 s

 configure
 router
 - mpls
 - shutdown
 - interface "system"
 no shutdown
 - exit
 - lsp "test"
 shutdown
 - exit
 - exit
 - rsvp
 shutdown
 interface "system"
 no shutdown
 - exit
 - exit
 exit
 exit

 Finished in 0.720 s
 </response>
 </item>
 <item>
 <admin>rollback compare</admin>
 <response>
0.160 s
0.070 s

 configure
 router
 - mpls
 - shutdown
 - interface "system"
 no shutdown
 -
```

```

- exit
- lsp "test"
- shutdown
- exit
- exit
- rsvp
- shutdown
- interface "system"
- no shutdown
- exit
- exit
- exit
service
- vpls "99" customer 1 create
- shutdown
- stp
- shutdown
- exit
- exit
- exit
exit

Finished in 0.350 s
 </response>
 </item>
</cli-action>
</data>
</rpc-reply>
]]>]]>

```

### Example 2 — Syntax error in the request resulting in global rpc-error reply:

```

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

```

### Reply:

```

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

```

```
</rpc-reply>
]]>]]>
```

### Example 3 — Error processing the request:

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

### Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
 <cli-action>
 <item>
 <admin>rollback compare active-cfg to 1</admin>
 </item>
 <response>
```

```
0.160 s
```

```
0.180 s
```

```

configure
router
- mpls
- shutdown
- interface "system"
- no shutdown
- exit
- exit
- rsvp
- shutdown
- interface "system"
- no shutdown
- exit
- exit
exit
exit

```

```
Finished in 0.460 s
```

```
 </response>
 </item>
 <item>
 <admin>rollback compare 1 to flee-fly</admin>
 <response>
 </response>
 <rpc-error>
 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>admin</err-element>
```

```

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

```

**Example 4** — Error in the 2nd item of the request, resulting in no 3rd item in the reply:

```

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

```

Reply:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="104" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
 <cli-action>
 <item>
 <admin>rollback compare active-cfg to 1</admin>
 </item>
 </cli-action>
 </data>
</rpc-reply>
</response>
0.170 s
1.350 s

configure
router
- mpls
- shutdown
- interface "system"
- no shutdown
- exit
- exit
- rsvp
- shutdown
- interface "system"
- no shutdown
- exit
- exit
- exit
exit

Finished in 1.640 s
 </response>
 </item>
 <item>

```

```

 <admin>rollback compare 1 to xyz</admin>
 <response>
 </response>
 <rpc-error>
 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>admin</err-element>
 </error-info>
 <error-message>
 command failed - '/admin rollback compare 1 to xyz'
 MINOR: CLI No such file ('xyz').
 </error-message>
 </rpc-error>
 </item>
</cli-action>
</data>
</rpc-reply>
]]>]]>

```

## System Provisioned Configuration (SPC) Objects

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

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

- In CLI these are removed by specifying the keyword 'no' which is then visible in an "info" command or in a saved config (admin save); for example, 'no log-id 99'.
- The Deletable SPC Objects can be removed or re-created via NETCONF <edit-config> requests, but they are not visible in a <get-config> response when they are:
  - Ø Set to their default values (including all child leaves & objects)
  - Ø Removed or deleted
- The Deletable SPC Objects are visible in a <get-config> response if a child leaf or object is changed away from the default value; for example, changing log-99 to time-format local.
- The list of Deletable SPC Objects as of 13.0.R1 is as follows:

```

Config system security profile default
Config system security profile default entry 10-100
Config system security profile administrative
Config system security profile administrative entry 10-112
Config system security user "admin"
Config system security user console member "default"
Config system security snmp view iso ...
Config system security snmp view li-view ...
Config system security snmp view mgmt-view ...
Config system security snmp view vprn-view ...
Config system security snmp view no-security-view ...
Config system security snmp access group xyz (a set of access groups)
Config system security ssh client-cipher-list protocol-version 1 cipher 200-210
Config system security ssh client-cipher-list protocol-version 2 cipher 190-235

```

```

Config system security ssh server-cipher-list protocol-version 1 cipher 200-205
Config system security ssh server-cipher-list protocol-version 2 cipher 190-235
Config log filter 1001
Config log filter 1001 entry 10
Config log log-id 99 & 100

```

Some SPC objects can't be deleted (Non-Deletable SPC Objects):

- There is no 'no' form in CLI
- The Non-Deletable SPC Objects are not visible in a <get-config> response when they are:
  - Ø Set to their default values (including all child leaves & objects)
  - Ø Removed or deleted
- The Non-Deletable SPC Objects are visible in a <get-config> response if a child leaf or object is changed away from the default value; for example, setting the card-type.
- The list of Non-Deletable SPC Objects as of 13.0.R1 is as follows:

```

Config system security user-template {tacplus_default|radius_default}
Config log event-control ...
Config filter log 101
Config qos ... various default policies can't be deleted
Config qos queue-group-templates ... these can't be deleted
Config card <x>
Config router network-domains network-domain "default"
Config oam-pm bin-group 1
Config call-trace trace-profile "default"

```

There are some Non-Deletable SPC Objects that are visible in a <get-config> request even if they are set to default values:

```

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

```

---

## Establishing a NETCONF Session

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

```
ssh -s my_username@192.168.0.92 -p 830 netconf
```

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

From the SR OS server:

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

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <capabilities>
 <capability>urn:ietf:params:netconf:base:1.0</capability>
 <capability>urn:ietf:params:netconf:base:1.1</capability>
 <capability>urn:ietf:params:netconf:capability:writable-running:1.0</capabil-
ity>
 <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
 <capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
 <capability>urn:ietf:params:netconf:capability:startup:1.0</capability>
 <capability>urn:ietf:params:netconf:capability:url:1.0?scheme=ftp,tftp,file</
capability>
 <capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-
mode=trim</capability>
 <capability>urn:ietf:params:xml:ns:netconf:base:1.0?module=ietf-net-
conf&revision=2015-02-27&features=writable-running, vali-
date, startup, url&deviations=alu-netconf-deviations-r13</capability>
 <capability>urn:alcatel-lucent.com:sros:ns:yang:netconf-deviations-r13?mod-
ule=alu-netconf-deviations-r13&revision=2015-02-27</capability>
 <capability>urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13?mod-
ule=alu-cli-content-layer-r13&revision=2015-02-27</capability>
 <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-r13?module=conf-
r13&revision=2015-02-27</capability>
 <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-aaa-r13?module=conf-aaa-
r13&revision=2015-02-27</capability>
 ...
 ...
 ...
 ...
 <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-vsm-r13?module=conf-vsm-
r13&revision=2015-02-27</capability>
 </capabilities>
 <session-id>54</session-id>
</hello>
]]>]]>
```

From a client:

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

---

## XML Content Layer

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

The XML formatted configuration information must be correctly ordered and has the same dependencies and behavior as the equivalent CLI commands.



## <edit-config> with XML Content Layer

An <edit-config> operation is supported with the <running> datastore only. The following <edit-config> operation attribute values are supported:

- merge
- remove
- delete
  - Ø A 'delete' operation for a leaf or a presence container will not return an error if the item is already deleted.
  - Ø An error is returned if attempting to delete a list node that doesn't exist.
  - Ø A 'delete' operation for a container without presence will return an error
- create
  - Ø A 'create' operation for a leaf or a presence container will not return an error if the item is being set to the same value.
  - Ø An error is returned if attempting to create a list node that already exists.
  - Ø A 'create' operation for a container without presence will result in an "OK" response (no error) but will be silently ignored.

'replace' is not supported as an attribute value for the <edit-config> operation.

Both 'delete' and 'remove' operations have the following behavior:

- Delete or remove operations are not supported for boolean leafs. For example, any of the following samples will return an error:
  - Ø <shutdown operation="delete"/>
  - Ø <shutdown operation="delete">false</shutdown>
  - Ø <interface operation="delete">
    - <interface-name>abc</interface-name>
    - <shutdown>true</shutdown>
</interface>
 (For this last case <shutdown operation="merge">true</shutdown> could be used instead to make the request valid.)
- A delete or remove operation is the equivalent of 'no xyz' in CLI. This 'no xyz' is applied whether the default for xyz is enabled ('xyz'), disabled ('no xyz') or some specific value. The delete operation is not aware of the default value of the object/leaf being deleted.
- A delete or remove for a leaf, where the request also specifies a value for the leaf, will result in an error.

The `<edit-config>` `<default-operation>` parameter is supported with the following values: merge, none. The 'replace' value is not supported. An operation of "none" on a leaf node (inherited or direct) causes that leaf statement to be ignored. No error will be returned if the leaf does not exist in the data model.

For 'merge' and 'create' operations the operations and tags specified in an `<edit-config>` request are order-aware and order-dependant and the sequence of operations must follow the required sequence of the equivalent CLI commands. The `<edit-config>` is processed and executed in a top-down order. The same leaf can be enabled, disabled, enabled and then disabled and the final result is whatever was last specified for that leaf in the `<edit-config>` request.

For 'delete' and 'remove' operations the SR OS NETCONF server will recursively "unwind" any children of the node being deleted or removed first before removing the node itself. The 'deepest' child branch of the request is examined first and any leafs are processed, after which the server works backwards out of the deepest branches back up to the object where the delete operation was specified. Note that if children branches of an object are required to be removed before deleting the object in CLI, then the equivalent delete request in a NETCONF `<edit-config>` must contain all those children if they exist, such as if the children are configured in the config datastore). For example:

```
<config>
 <configure>
 <service>
 <vp1s operation="delete">
 <service-id>11</service-id>
 <interface>
 <ip-int-name>test</ip-int-name>
 <shutdown operation="merge">true</shutdown>
 </interface>
 <shutdown operation="merge">true</shutdown>
 </vp1s>
 </service>
 </configure>
</config>
```

In the example above, SR OS will first shutdown the test interface, then delete the interface, then shutdown the VPLS and then finally remove it.

Note that the 'operation="merge"' is required in the shutdown nodes because otherwise the inherited operation is delete which is not supported on boolean leafs.

If other children of vp1s 11 exist in the config besides the interface 'test' specified in the delete request above, and those children are required in CLI to be deleted before removing vp1s 11, then the deletion request above will fail. All configured children must be specified in the delete request.

## **`<get-config>` with XML Content Layer**

A `<get-config>` operation is supported with the `<running>` datastore only.

Subtree filtering for basic subtree selection is supported for XML content layer `<get-config>` requests. Post-filtering of the selected subtrees is not supported. The details of subtree filter support are as follows:

- Attribute match expressions (section 6.2.2 of RFC 6241) are not supported. See details below about content match nodes.
- Only containers are supported as selection nodes (section 6.2.4 of RFC 6241). Empty leaf nodes or list name nodes are not supported as selection nodes.
  - Ø Nodes that represent lists must also include content match nodes for all keys of the list; for example, `<configure><router><interface><interface-name>abc</interface-name>`.
  - Ø A selection node that is a list, without also specifying the key, is not supported; for example, `<configure><router><interface/>` is not supported. An alternative is to request the parent containment node that contains the desired list node; for example, `<configure><router>` instead of `<configure><router><interface/>`.
- Content match nodes (section 6.2.5 of RFC 6241) are only supported for key leafs; for example, `<configure><router><interface><interface-name>abc</interface-name>`.
  - Ø Content match nodes that are leafs but are not also keys will result in an error (not silently ignored).

**Example 1** — The following request will return an error:

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

Reply:

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

```

 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>get-config</err-element>
 </error-info>
 <error-message>
 command failed - 'configure router interface "abc" delayed-enable'
 </error-message>
 </rpc-error>
</rpc-reply>
]]>]]>

```

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

**Example 2** — A valid `<get-config>` request (content match on a list key):

```

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

```

**Example 3** — A valid `<get-config>` request (selection node that is a container):

```

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

```

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

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

**Example 4** — An invalid <get-config> request (list name node - invalid selection node):

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

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <rpc-error>
 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>get-config</err-element>
 </error-info>
 <error-message>
 command failed - 'configure router interface'
 </error-message>
 </rpc-error>
</rpc-reply>
]]>]]>
```

**Example 5** — An invalid <get-config> request (empty leaf node - invalid selection node):

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

```

 <ftp-server>
 </ftp-server>
 </security>
 </system>
 </configure>
 </filter>
 </get-config>
</rpc>
]]>]]>

```

Reply:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <rpc-error>
 <error-type>protocol</error-type>
 <error-tag>bad-element</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <bad-element>ftp-server</bad-element>
 </error-info>
 <error-message>
 Element is not valid in the specified context.
 </error-message>
 </rpc-error>
</rpc-reply>
]]>]]>

```

**Example 6** — An invalid <get-config> request (key repeated in the same instance of the list node):

```

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

```

Reply:

```

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

```

```

 <error-type>application</error-type>
 <error-tag>operation-failed</error-tag>
 <error-severity>error</error-severity>
 <error-info>
 <err-element>get-config</err-element>
 </error-info>
 <error-message>
 command failed - 'configure router interface "abc" "def"'
 </error-message>
 </rpc-error>
</rpc-reply>
]]>]]>

```

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

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

Example:

```

<get-config>
 <source>
 <running/>
 </source>
</get-config>

```

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

Example:

```

<get-config>
 <source>
 <running/>
 </source>
 <filter>
 <configure/>
 </filter>
</get-config>

```

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

## XML Content Layer Examples

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

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

```

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

```

## XML Content Layer Examples

```
<source> <running/> </source>
<filter>
 <configure>
 <system>
 <netconf>
 </netconf>
 </system>
 </configure>
 </filter>
</get-config>
</rpc>
]]>]]>
```

### Reply:

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

Below is an example of a <edit-config> request and response to create a basic VPRN service:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
 xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <edit-config>
 <target>
 <running/>
 </target>
 <config>
 <configure>
 <service>
 <vprn operation="create">
 <service-id>200</service-id>
 <customer>1</customer>
 </vprn>
 </service>
 </configure>
 </config>
 </edit-config>
</rpc>
]]>]]>
```

### Reply:

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



```

 <ok/>
 </rpc-reply>
]>]]>

```

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

```

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

```

Reply:

```

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

```

---

## CLI Content Layer

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

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

### Example 1:

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

### Example 2:

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

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

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

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

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

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

For more information, see "CLI Content Layer Examples".

## CLI Content Layer Examples

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

Below is an example of a config change request and response. Note that 'exit all' at the beginning of the CLI block is not required (it is automatically assumed by the SR OS NETCONF server).

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

Reply:

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

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

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

Reply:

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

 #-----
 echo "IP Configuration"
 #-----
 interface "system"
 no shutdown
 exit

 </response>
 </item>
 <item>
 <cli-info-detail>system login-control</cli-info-detail>
 <response>

 ftp
 inbound-max-sessions 3
 exit
 ssh
 no disable-graceful-shutdown
 inbound-max-sessions 5
 outbound-max-sessions 5
 no ttl-security
 exit
 telnet
 no enable-graceful-shutdown
 inbound-max-sessions 5
 outbound-max-sessions 5
 no ttl-security
 exit
 idle-timeout 30
 no pre-login-message
 no motd
 login-banner
 no exponential-backoff

 </response>
 </item>
 </config-format-cli-block>
 </data>
 </rpc-reply>
]>]]>
```

Below is an example of a <get-config> request and response to retrieve full configuration information. Note that <cli-info-detail/> can be used to get the full configuration including default settings.

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

### Reply:

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

Generated WED JAN 07 01:07:43 2015 UTC

exit all
configure
#-----
echo "System Configuration"
#-----
 system
 chassis-mode d
 dns
 exit
 load-balancing
 lsr-load-balancing lbl-ip
 system-ip-load-balancing
 exit
 netconf
 no shutdown
 exit
 snmp
 shutdown
 engineID "deadbeefdeadbeef"
 exit
 time
 ntp
 authentication-key 1 key "OAwgNULbzgI" hash2 type des
 no shutdown
 exit
 sntp
 shutdown
 exit
```

```

 zone EST
 exit
 thresholds
 rmon
 exit
 exit
#-----
echo "Cron Configuration"
#-----
 cron
 ...
 ...
 ...
 exit
 exit
#-----
echo "System Security Configuration"
#-----
 ...
 ...
 ...
#-----
echo "System Time NTP Configuration"
#-----
 system
 time
 ntp
 exit
 exit
 exit

exit all

Finished WED JAN 07 01:07:43 2015 UTC

</response>
</item>
</config-format-cli-block>
</data>
</rpc-reply>
]]>]]>

```

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

```

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

```

Reply:

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

```
=====
SSH Server
=====
```

```
Administrative State : Enabled
Operational State : Up
Preserve Key : Enabled

SSH Protocol Version 1 : Disabled

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

```

Connection Username
 Version Cipher ServerName Status

135.121.143.254 admin
 2 aes128-cbc netconf connected

```

```
Number of SSH sessions : 1
=====
```

```
 </response>
 </item>
 </oper-data-format-cli-block>
</data>
</rpc-reply>
]]>]]>
```





---

# NETCONF Command Reference

---

## Command Hierarchies

### Configuration Commands

#### NETCONF System Commands

```

config
 — system
 — netconf
 — [no] shutdown

```

#### NETCONF Security Commands

```

config
 — system
 — security
 — user user-id
 — access [ftp] [snmp] [console] [li][netconf]

```

```

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

```

#### Show Commands

```

show
 — system
 — netconf
 — counters

```



---

## Configuration Commands

---

### NETCONF System Commands

---

#### netconf

<b>Syntax</b>	<b>netconf</b>
<b>Context</b>	config>system>security>profile
<b>Description</b>	This command authorizes netconf capability for the user.

#### kill-session

<b>Syntax</b>	<b>[no] kill-session</b>
<b>Context</b>	config>system>security>profile>netconf>base-op-authorization
<b>Description</b>	This operation authorizes a user associated with the profile to send a <kill-session> NETCONF operation. This <kill-session> operation allows a NETCONF client to kill another NETCONF session, but not the session in which the operation is requested.
<b>Default</b>	<b>no kill-session</b>

#### shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>netconf
<b>Description</b>	This command disables the NETCONF server. 'shutdown' is blocked if there are any active NETCONF sessions. Use the “admin disconnect” command to disconnect all NETCONF sessions before shutting down the NETCONF service.

#### base-op-authorization

<b>Syntax</b>	<b>base-op-authorization</b>
<b>Context</b>	config>system>security>profile>netconf
<b>Description</b>	This command authorizes a user associated with the profile to send a <kill-session> NETCONF operation.



---

## Show Commands

---

### NETCONF System Commands

---

#### netconf

**Syntax**    **netconf**

**Context**    show>system

**Description**    This command displays NETCONF SSH sessions.

**Output**    **SSH Options Output** — The following table describes NETCONF output fields .

Label	Description
Administrative State	Enabled — Displays that NETCONF is enabled. Disabled — Displays that NETCONF is disabled.
Operational State	Up — Displays that NETCONF is operational. Down — Displays that NETCONF is not operational.
Connection	The IP address of the connected router(s) (remote client).
Username	The name of the user.
Session ID	The NETCONF session ID.
Status	Connected or not connected.
Number of sessions	Total NETCONF sessions

```
*A:bksim3107# show system netconf

=====
NETCONF Server
=====
Administrative State : Enabled
Operational State : Up

Connection Username Session Status
 Id

192.168.7.229 admin 1 connected
192.168.7.229 test1 2 connected
192.168.7.229 test2 3 connected

Number of NETCONF sessions : 3
=====
```

counters

- Syntax** counters
- Context** show>system>netconf
- Description** This command displays NETCONF counters.
- Output** **SSH Options Output** — The following table describes NETCONF counter output fields .

Label		Description
RX Messages		Types and numbers of receive messages
Total RX		Total of all receive messages
TX Messages		Types and numbers of send messages
Total TX		Total of all send messages

```
*A:bksim3107# show system netconf counters
```

```
=====
```

```
NETCONF counters:
```

```
=====
```

```
Rx Messages
```

```

```

in gets	: 0
in get-configs	: 0
in edit-configs	: 0
in close-sessions	: 0
in kill-sessions	: 0

```

```

Rx Total	: 0
----------	-----

```
=====
```

```
Tx Messages
```

```

```

out rpc-errors	: 0
----------------	-----

```

```

Tx Total	: 0
----------	-----

```
=====
```





# Event and Accounting Logs

---

## In This Chapter

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

Topics in this chapter include:

- [Logging Overview on page 378](#)
- [Log Destinations on page 380](#)
- [Event Logs on page 385](#)
  - [Event Sources on page 386](#)
  - [Event Control on page 387](#)
  - [Log Manager and Event Logs on page 389](#)
  - [Event Filter Policies on page 390](#)
  - [Event Log Entries on page 391](#)
  - [Simple Logger Event Throttling on page 393](#)
  - [Default System Log on page 394](#)
  - [Event Handling System on page 394](#)
- [Accounting Logs on page 396](#)
  - [Accounting Records on page 396](#)
  - [Accounting Files on page 412](#)
  - [Design Considerations on page 412](#)
- [Configuration Notes on page 418](#)

## Logging Overview

The two primary types of logging supported in the 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 OS groups events into three major categories or event sources:

- Security events — Events that pertain to attempts to breach system security.
- Change events — Events that pertain to the configuration and operation of the node.
- Main events — Events that pertain to applications that are not assigned to other event categories/sources.
- Debug events — Events that pertain to trace or other debugging information.

The following are events within the 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 OS conform to ITU standards M.3100 X.733 & X.21 and are listed in [Table 37](#).

**Table 37: 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 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 OS 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. routers support the following log destinations:

- [Console on page 380](#)
- [Session on page 380](#)
- [Memory Logs on page 380](#)
- [Log Files on page 381](#)
- [SNMP Trap Group on page 383](#)
- [Syslog on page 383](#)

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 “to session” configuration is removed. Event logs configured with a session destination are stored in the configuration file but the “to session” part is not stored. 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 ee ff -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 aa \overline{ff} -timestamp.xml.gz
```

where:

*aa* is the accounting policy ID

*ff* is the log file destination ID

*timestamp* is the timestamp when the file is created in the form of *yyyymmdd-hhmmss*

where:

*yyyy* is the four-digit year (for example, 2007)

*mm* is the two digit number representing the month (for example, 12 for December)

*dd* is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

*hh* is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

*mm* is the two digit minute (for example, 30 for 30 minutes past the hour)

*ss* is the two digit second (for example, 14 for 14 seconds)

Accounting logs are .xml files created in a compressed format and have a .gz extension.

The **\act-collect** directory is where active accounting logs are written. When an accounting log is rolled over, the active file is closed and archived in the **\act** directory before a new active accounting log file created in **\act-collect**.

## SNMP Trap Group

An event log can be configured to send events to SNMP trap receivers by specifying an SNMP trap group destination.

An SNMP trap group can have multiple trap targets. Each trap target can have different operational parameters.

A trap destination has the following properties:

- The IP address of the trap receiver.
- The UDP port used to send the SNMP trap.
- SNMP version (v1, v2c, or v3) used to format the SNMP notification.
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

For SNMP traps that will be sent 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 router.

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 router uses six internal severity levels, the severity levels are mapped to syslog severities. [Table 38](#) displays the severity level mappings to syslog severities.

**Table 38: Router to Syslog Severity Level Mappings**

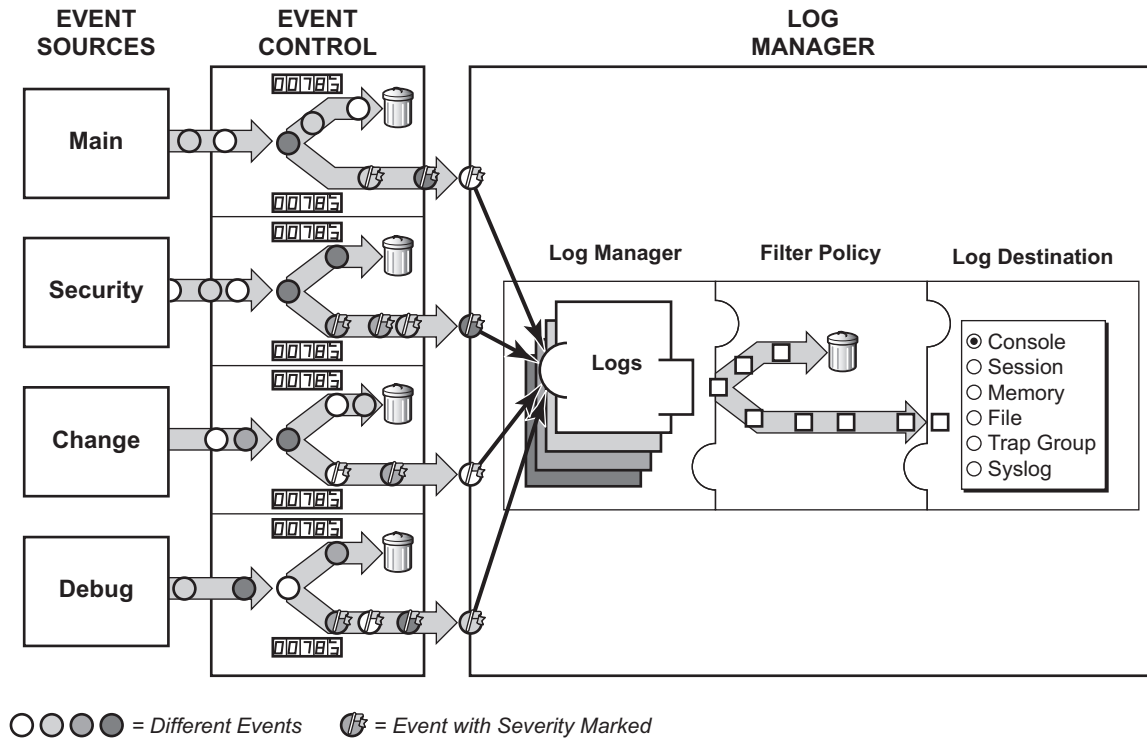
Severity Level	Numerical Severity (highest to lowest)	Syslog Configured Severity	Definition
	0	emergency	System is unusable
3	1	alert	Action must be taken immediately
4	2	critical	Critical conditions
5	3	error	Error conditions
6	4	warning	Warning conditions
	5	notice	Normal but significant condition
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 router.

Figure 10 depicts a function block diagram of event logging.



CLI0001B

Figure 10: Event Logging Block Diagram

## Event Sources

In [Figure 10](#), the event sources are the main categories of events that feed the log manager.

- **Security** — The security event source is all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the SECURITY application and the authenticationFailure event in the SNMP application.
- **Change** — The change activity event source is all events that directly affect the configuration or operation of the node. Change events are generated by the USER application. The Change event stream also includes the tmnxConfigModify (#2006), tmnxConfigCreate (#2007), tmnxConfigDelete (#2008) and tmnxStateChange (#2009) change events from the SYSTEM application.
- **Debug** — The debug event source is the debugging configuration that has been enabled on the system. Debug events are generated by the DEBUG application.
- **Main** — The main event source receives events from all other applications within the router.

Examples of applications within the system include IP, MPLS, OSPF, CLI, services, etc. The following example displays a partial sample of the **show log applications** command output which displays all applications.

```
*A:ALA-48# show log applications
=====
Log Event Application Names
=====
Application Name

...
BGP
CCAG
CFLOWD
CHASSIS
...
MPLS
MSDP
NTP
...
TOD
USER
VRRP
VRTR
=====
*A:ALA-48#
```

## 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 393](#).

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

CCAG:
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 sapTlsDHCPLeaseStEntriesExceeded WA gen 0 0
 2003 sapTlsDHCPLeaseStateOverride WA gen 0 0
...
DEBUG:
L 2001 traceEvent MI gen 0 0
DOTIX:
FILTER:
 2001 filterPBRPacketsDropped MI 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
 2002 vRtrIsisManualAddressDrops WA gen 0 0
```

## Event Control

2003	vRtrIisisCorruptedLSPDetected	WA	gen	0	0	
...						
LAG:						
2001	DynamicCostOn	WA	gen	0	0	
2002	DynamicCostOff	WA	gen	0	0	
2003	LagPortAddFailed	WA	gen	0	0	
LDP:						
2001	vRtrLdpStateChange	MI	gen	0	0	
2002	vRtrLdpInstanceStateChange	MI	gen	0	0	
2003	vRtrLdpIfStateChange	MI	gen	0	0	
...						
LOGGER:						
L	2001	STARTED	MI	gen	4	0
L	2002	traceErrorEvent	CR	gen	0	0
	2005	tmnxLogSpaceContention	MA	gen	0	0
...						
MIRROR:						
	2001	sourceEnabled	MI	gen	0	0
	2002	sourceDisabled	MI	gen	0	0
	2003	destinationEnabled	MI	gen	0	0
...						
MPLS:						
	2001	mplsXCUp	WA	gen	0	0
	2002	mplsXCDown	WA	gen	0	0
	2003	mplsTunnelUp	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 7450 ESS, 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 39](#):

**Table 39: 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 40](#).

**Table 40: Log Entry Field Descriptions**

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

**Table 40: Log Entry Field Descriptions (Continued)**

Label	Description
<severity>	<p>The severity level name of the event.</p> <p>CLEARED — A cleared event (severity number 1).</p> <p>INFO — An indeterminate/informational severity event (severity level 2).</p> <p>CRITICAL — A critical severity event (severity level 3).</p> <p>MAJOR — A major severity event (severity level 4).</p> <p>MINOR — A minor severity event (severity level 5).</p> <p>WARNING — A warning severity event (severity 6).</p>
<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#
```

## Event Handling System

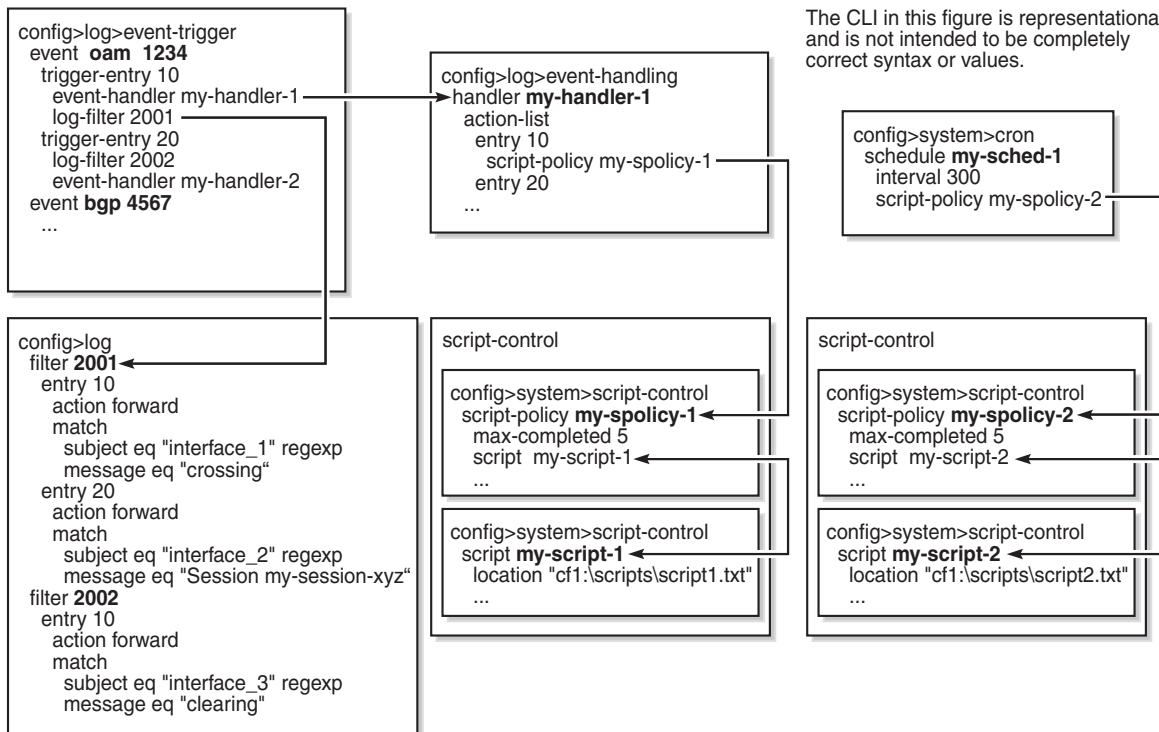
The Event Handling System (EHS) is a tool that allows operator-defined behavior to be configured on the router. EHS adds user-controlled programmatic exception handling by allowing a CLI script to be executed upon the detection of a log event (the 'trigger'). Regexp style expression matching is available on various fields in the log event to give flexibility in the trigger definition.

EHS handler objects are used to tie together:

- trigger events (typically log events that match some configurable criteria)
- a set of actions to perform (typically one or more CLI scripts)

EHS, along with CRON, makes use of the generic SR OS CLI script-control functions for scripts. Any command available in CLI (with some limited exceptions such as 'candidate' commands) can be executed in a script as the result of an EHS handler being triggered.

The following figure illustrates the relationships between the different configurable objects used by EHS (and CRON).



24884

**Figure 11: EHS Object Relationships**

Complex rules can be configured to match on log events as a trigger for an EHS handler.

When a log event is generated in SR OS it will be subject to discard via suppression and throttling (**config>log>event-control**) before it is evaluated as a trigger for EHS:

- EHS will not trigger on log events that are suppressed through **config>log>event-control**
- EHS will not trigger on log events that are throttled by the logger

EHS will trigger on log events that are dropped by user configured log filters that are assigned to individual logs (**config>log>filter**). The EHS event trigger logic occurs before the distribution of log event streams into individual logs.

## 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 43](#), [Table 44](#), and [Table 45](#) provide field descriptions.

**Table 41: 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-network-ingr-egr	cpNipo & cpNepo	Network port	15
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
custom-record-aa-sub	aaSubCustom	AA subscriber	15

**Table 41: Accounting Record Name and Collection Periods (Continued)**

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
combined-mpls-lsp-egress	mplsLspEgr	LSP	5
combined-mpls-lsp-ingress	mplsLspIn	LSP	5
saa	saa png trc hop	SAA or SAA test	5
complete-ethernet-port	enet	Ethernet port	15

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.

Refer to the Application Assurance Statistics Fields Generated per Record table in the 7450 ESS-Series OS Integrated Services Adapter Guide for fields names for Application Assurance records.

**Table 42: 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
Service-egress-octets (seo) (**)	seo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 42: Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
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
Network-ingress-packets (nip)	nip	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped

**Table 42: Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
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 42: 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 42: Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-network-ingr-egr (cpNipo & cpNepo)	cpNipo	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
	cpNepo	port	PortId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 42: 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 42: 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
		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 42: 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
		v4pf	IPv4PktsForwarded
		v6pf	IPv6PktsForwarded
		v4pd	IPv4PktsDropped
		v6pd	IPv6PktsDropped
		v4of	IPv4OctetsForwarded
		v6of	IPv6OctetsForwarded
		v4od	IPv4OctetsDropped
		v6od	IPv6OctetsDropped
	cpSBepo	qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 42: Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
		v4pf	IPv4PktsForwarded
		v6pf	IPv6PktsForwarded
		v4pd	IPv4PktsDropped
		v6pd	IPv6PktsDropped
		v4of	IPv4OctetsForwarded
		v6of	IPv6OctetsForwarded
		v4od	IPv4OctetsDropped
		v6od	IPv6OctetsDropped

**Table 42: 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 42: 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

**Table 42: Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-ethernet-port (enet)	enet	port	PortId
		to	EtherStatsOctets
		tp	EtherStatsPkts
		de	EtherStatsDropEvents
		tbcp	EtherStatsBroadcastPkts
		mcp	EtherStatsMulticastPkts
		cae	EtherStatsCRCAlignErrors
		up	EtherStatsUndersizePkts
		op	EtherStatsOversizePkts
		fgm	EtherStatsFragments
		jab	EtherStatsJabbers
		col	EtherStatsCollisions
		p64o	EtherStatsPkts64Octets
		p127o	EtherStatsPkts65to127Octets
		p255o	EtherStatsPkts128to255Octets
		p511o	EtherStatsPkts256to511Octets
		p1023o	EtherStatsPkts512to1023Octets
		p1518o	EtherStatsPkts1024to1518Octets
		po1518o	EtherStatsPktsOver1518Octets
		ae	Dot3StatsAlignmentErrors
		fe	Dot3StatsFCSErrors
		scf	Dot3StatsSingleCollisionFrames
		mcf	Dot3StatsMultipleCollisionFrames
		sqe	Dot3StatsSQETestErrors
		dt	Dot3StatsDeferredTransmissions
		lcc	Dot3StatsLateCollisions
		exc	Dot3StatsExcessiveCollisions
		imt	Dot3StatsInternalMacTransmitErrors
		cse	Dot3StatsCarrierSenseErrors
		ftl	Dot3StatsFrameTooLongs
		imre	Dot3StatsInternalMacReceiveErrors
		se	Dot3StatsSymbolErrors
		ipf	Dot3InPauseFrames
		opf	Dot3OutPauseFrames

(\*) 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 7450 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 43](#), [Table 44](#), and [Table 45](#) provide field descriptions.

**Table 43: 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 43: Policer Stats Field Descriptions (Continued)**

Field	Field Description
oof	OutOfProfileOctetsForwarded
ooo	OutOfProfileOctetsOffered
uco	UncoloredOctetsOffered
v4po	IPv4PktsOffered *
v4oo	IPv4OctetsOffered *
v6po	IPv6PktsOffered *
v6oo	IPv6OctetsOffered *
v4pf	IPv4PktsForwarded *
v6pf	IPv6PktsForwarded *
v4pd	IPv4PktsDropped *
v6pd	IPv6PktsDropped *
v4of	IPv4OctetsForwarded *
v6of	IPv6OctetsForwarded *
v4od	IPv4OctetsDropped *
v6od	IPv6OctetsDropped *

\* Enhanced Subscriber Management (ESM) only.

**Table 44: Queue Group Record Types**

Record Name	Description
qgone	PortQueueGroupOctetsNetworkEgress
qgosi	PortQueueGroupOctetsServiceIngress
qgoese	PortQueueGroupOctetsServiceEgress
qgpne	PortQueueGroupPacketsNetworkEgress
qgpsi	PortQueueGroupPacketsServiceIngress
qgpse	PortQueueGroupPacketsServiceEgress
fpqgosi	ForwardingPlaneQueueGroupOctetsServiceIngress
fpqgoni	ForwardingPlaneQueueGroupOctetsNetworkIngress
fpqgpsi	ForwardingPlaneQueueGroupPacketsServiceIngress
fpqgpni	ForwardingPlaneQueueGroupPacketsNetworkIngress

**Table 45: 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

**Table 45: Queue Group Record Type Fields (Continued)**

Field	Field Description
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 router 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 381](#).

## Design Considerations

The router 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 415](#)
  - [RADIUS Accounting in Networks Using ESM on page 415](#)
- 

### 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.

---

## 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.

---

### AA Accounting per Forwarding Class

This feature allows the operator to report on protocol/application/app-group volume usage per forwarding class by adding a bitmap information representing the observed FC in the XML accounting files. 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 on page 420](#)  
→ [Log Types on page 420](#)
- [Basic Event Log Configuration on page 421](#)
- [Common Configuration Tasks on page 422](#)
- [Log Management Tasks on page 440](#)

## 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 "ospf" 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 424](#)
  - [Configuring an Event Log on page 422](#)
  - [Configuring an Accounting Policy on page 425](#)
  - [Configuring Event Control on page 426](#)
  - [Configuring a Log Filter on page 428](#)
  - [Configuring an SNMP Trap Group on page 429](#)
  - [Configuring a Syslog Target on page 437](#)
- 

## Configuring an Event Log

An event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

**CLI Syntax:**

```
config>log
log-id log-id
description description-string
filter filter-id
from {[main] [security] [change] [debug-trace]}
to console
to file file-id
to memory [size]
to session
to snmp [size]
to syslog syslog-id}
time-format {local|utc}
no shutdown
```

The following displays a log file configuration example:

```
ALA-12>config>log>log-id# info

...
 log-id 2
 description "This is a test log file."
 filter 1
 from main security
 to file 1
 exit
...

ALA-12>config>log>log-id#
```

## Configuring a File ID

To create a log file a file ID is defined, 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 cfl:
 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 422](#) and [Configuring a File ID on page 424](#).

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 "bgp" 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 [regex]
 severity {eq|neq|lt|lte|gt|gte} severity-level
 subject {eq|neq} subject [regex]
```

The following displays a log filter configuration example:

```
A:ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
 file-id 1
 description "This is our log file."
 location cfl:
 rollover 600 retention 24
 exit
 filter 1
 default-action drop
 description "This is a sample filter."
 entry 1
 action forward
 match
 application eq "mirror"
 severity eq critical
 exit
 exit
 exit
...
 log-id 2
 shutdown
 description "This is a test log file."
 filter 1
 from main security
 to file 1
 exit
...
#-----
A:ALA-12>config>log#
```

## Configuring an SNMP Trap Group

The associated *log-id* does not have to be configured before a **snmp-trap-group** can be created, however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

Use the following CLI syntax to configure an SNMP trap group:

**CLI Syntax:**

```
config>log
 snmp-trap-group log-id
 trap-target name [address ip-address] [port port]
 [snmpv1|snmpv2c| snmpv3] notify-community communi-
 tyName |snmpv3SecurityName [security-level {no-
 auth-no-privacy|auth-no-privacy|privacy}] [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#
```

## Configuring an SNMP Trap Group

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#
```

## Configuring an 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
administrative 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#
```

## Configuring an SNMP Trap Group

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
administrative 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
=====
```

## Configuring an SNMP Trap Group

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 administrative 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|info|debug}
 facility syslog-facility
```

The following displays a syslog configuration example:

```
A:ALA-12>config>log# info

...
 syslog 1
 description "This is a syslog file."
 address 10.10.10.104
 facility user
 level warning
 exit
...

A:ALA-12>config>log#
```

## 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#
```

The following is an example custom record configuration.

```
Dut-C>config>log>acct-policy>cr# info

 aa-specific
 aa-sub-counters
 short-duration-flow-count
 medium-duration-flow-count
 long-duration-flow-count
 total-flow-duration
 total-flows-completed-count
 exit
 from-aa-sub-counters
 flows-admitted-count
 flows-denied-count
 flows-active-count
 packets-admitted-count
 octets-admitted-count
 packets-denied-count
 octets-denied-count
 max-throughput-octet-count
```

```
max-throughput-packet-count
max-throughput-timestamp
forwarding-class
exit
to-aa-sub-counters
flows-admitted-count
flows-denied-count
flows-active-count
packets-admitted-count
octets-admitted-count
packets-denied-count
octets-denied-count
max-throughput-octet-count
max-throughput-packet-count
max-throughput-timestamp
forwarding-class
exit
exit
significant-change 1
ref-aa-specific-counter any

```

## Log Management Tasks

This section discusses the following logging tasks:

- [Modifying a Log File on page 441](#)
- [Deleting a Log File on page 443](#)
- [Modifying a File ID on page 444](#)
- [Deleting a File ID on page 445](#)
- [Modifying a Syslog ID on page 446](#)
- [Deleting a Syslog on page 446](#)
- [Modifying an SNMP Trap Group on page 447](#)
- [Deleting an SNMP Trap Group on page 448](#)
- [Modifying a Log Filter on page 448](#)
- [Deleting a Log Filter on page 450](#)
- [Modifying Event Control Parameters on page 450](#)
- [Returning to the Default Event Control Configuration on page 451](#)



## 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
```

## Modifying a Log File

The following displays the modified log file configuration:

```
A:ALA-12>config>log# info

...
 log-id 2
 description "Chassis log file."
 filter 2
 from security
 to file 1
 exit
...

A:ALA-12>config>log#
```

## Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, **file 1** is associated with **log-id 2**.

```
A:ALA-12>config>log# info

 file-id 1
 description "LocationTest."
 location cfl:
 rollover 600 retention 24
 exit
...
 log-id 2
 description "Chassis log file."
 filter 2
 from security
 to file 1
 exit
...

A:ALA-12>config>log#
```

Use the following CLI syntax to delete a log file:

**CLI Syntax:**

```
config>log
 no log-id log-id
 shutdown
```

The following displays an example to delete a log file:

**Example:**

```
config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

## Modifying a File ID

**NOTE:** When the **file-id** location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear>log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log not cleared, the old location remains in effect.

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|info|debug}
 facility syslog-facility
```

The following displays an example of the syslog ID modifications:

**Example:**

```
config# log
config>log# syslog 1
config>log>syslog$ description "Test syslog."
config>log>syslog# address 10.10.0.91
config>log>syslog# facility mail
config>log>syslog# level info
```

The following displays the syslog configuration:

```
A:ALA-12>config>log# info

...
 syslog 1
 description "Test syslog."
 address 10.10.10.91
 facility mail
 level info
 exit
...

A:ALA-12>config>log#
```

## Deleting a Syslog

Use the following CLI syntax to delete a syslog file:

**CLI Syntax:**

```
config>log
 no syslog syslog-id
```

The following displays an example to delete a syslog ID:

**Example:** config# log  
 config>log# no syslog 1

## Modifying an SNMP Trap Group

Use the following CLI syntax to modify an SNMP trap group:

**CLI Syntax:** config>log  
                   snmp-trap-group log-id  
                   trap-target name [address ip-address] [port port] [sn-  
                                   mpv1|snmpv2c| snmpv3] notify-community communi-  
                                   tyName |snmpv3SecurityName [security-level {no-  
                                   auth-no-privacy|auth-no-privacy|privacy}]

The following displays the current SNMP trap group configuration:

```
A:ALA-12>config>log# info

...
 snmp-trap-group 10
 trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
 exit
...

A:ALA-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

**Example:** config# log  
 config>log# snmp-trap-group 10  
 config>log>snmp-trap-group# no trap-target 10.10.10.104:5  
 config>log>snmp-trap-group# snmp-trap-group# trap-target  
 10.10.0.91:1 snmpv2c notify-community "com1"

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info

...
 snmp-trap-group 10
 trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
 exit
...

A:ALA-12>config>log#
```

## Deleting an SNMP Trap Group

Use the following CLI syntax to delete a trap target and SNMP trap group:

**CLI Syntax:** config>log  
no snmp-trap-group *log-id*  
no trap-target *name*

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info

...
 snmp-trap-group 10
 trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
 exit
...

A:ALA-12>config>log#
```

The following displays an example to delete a trap target and an SNMP trap group.

**Example:** config>log# snmp-trap-group 10  
config>log>snmp-trap-group# no trap-target 10.10.0.91:1  
config>log>snmp-trap-group# exit  
config>log# no snmp-trap-group 10

## Modifying a Log Filter

Use the following CLI syntax to modify a log filter:

**CLI Syntax:** config>log  
filter *filter-id*  
default-action {drop|forward}  
description *description-string*  
entry *entry-id*  
action {drop|forward}  
description *description-string*  
match  
application {eq|neq} *application-id*  
number {eq|neq|lt|lte|gt|gte} *event-id*  
router {eq|neq} *router-instance* [regex]  
severity {eq|neq|lt|lte|gt|gte} *severity-level*  
subject {eq|neq} *subject* [regex]



The following output displays the current log filter configuration:

```
ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
...
 filter 1
 default-action drop
 description "This is a sample filter."
 entry 1
 action forward
 match
 application eq "mirror"
 severity eq critical
 exit
 exit
 exit
...

ALA-12>config>log#
```

The following displays an example of the log filter modifications:

**Example:**

```
config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
A:ALA-12>config>log>filter# info

...
 filter 1
 description "This allows <n>."
 entry 1
 action drop
 match
 application eq "user"
 number eq 2001
 exit
 exit
 exit
...

A:ALA-12>config>log>filter#
```

## Deleting a Log Filter

Use the following CLI syntax to delete a log filter:

**CLI Syntax:** `config>log  
no filter filter-id`

The following output displays the current log filter configuration:

```
A:ALA-12>config>log>filter# info

...
 filter 1
 description "This allows <n>."
 entry 1
 action drop
 match
 application eq "user"
 number eq 2001
 exit
 exit
 exit
 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 "ospf" 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 ospf 2014 suppress

The following displays the log filter configuration:

```
A:ALA-12>config>log# info

...
event-control "ospf" 2014 suppress
...

A:ALA-12>config>log#
```

## Returning to the Default Event Control Configuration

The **no** form of the **event-control** command returns modified values back to the default values.

Use the following CLI syntax to modify event control parameters:

**CLI Syntax:** config>log  
 no event-control application [event-name |event-number]

The following displays an example of the command usage to return to the default values:

**Example:** config# log  
 config>log# no event-control "ospf" 2001  
 config>log# no event-control "ospf" 2002  
 config>log# no event-control "ospf" 2014

```
A:ALA-12>config>log# info detail

#-----
echo "Log Configuration"
#-----
event-control "ospf" 2001 generate minor
event-control "ospf" 2002 generate warning
event-control "ospf" 2003 generate warning
event-control "ospf" 2004 generate critical
event-control "ospf" 2005 generate warning
event-control "ospf" 2006 generate warning
event-control "ospf" 2007 generate warning
event-control "ospf" 2008 generate warning
event-control "ospf" 2009 generate warning
```

## Returning to the Default Event Control Configuration

```
event-control "ospf" 2010 generate warning
event-control "ospf" 2011 generate warning
event-control "ospf" 2012 generate warning
event-control "ospf" 2013 generate warning
event-control "ospf" 2014 generate warning
event-control "ospf" 2015 generate critical
event-control "ospf" 2016 generate warning
...

A:ALA-12>config>log#
```

---

# Log Command Reference

---

## Command Hierarchies

- [Log Command Reference on page 453](#)
  - [Accounting Policy Commands on page 454](#)
  - [Custom Record Commands on page 455](#)
  - [File ID Commands on page 458](#)
  - [Event Filter Commands on page 458](#)
  - [Event Handling System \(EHS\) Commands on page 459](#)
  - [Event Trigger Commands on page 459](#)
  - [Log ID Commands on page 460](#)
  - [SNMP Trap Group Commands on page 460](#)
  - [Syslog Commands on page 461](#)
- [Show Commands on page 462](#)
- [Clear Command on page 462](#)

## Log Configuration Commands

```

config
 — log
 — app-route-notifications
 — [no] cold-start-wait
 — [no] route-recovery-wait
 — event-control application-id [event-name | event-number] [generate [severity-level] [throt-

tle] [specific-throttle-rate events-limit interval seconds] [disable-specific-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
 — [no] include-router-info
 — [no] include-system-info
 — 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
 — all
 — [no] flows-active-count [all]
 — [no] flows-admitted-count
 — [no] flows-denied-count
 — [no] forwarding-class
 — [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] forwarding-class
 — [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

Refer to the 7x50 SR OS Services Guide for information about configuring log filters in a VPRN service.

```

config
 — log
 — [no] filter filter-id
 — default-action {drop | forward}
 — no default-action
 — description description-string
 — no description
 — [no] entry entry-id
 — action {drop | forward}
 — no action
 — description description-string
 — no description
 — [no] match
 — application {eq | neq} application-id
 — no application
 — message {eq | neq} pattern [regexp]
 — no message
 — number {eq | neq | lt | lte | gt | gte} event-id
 — no number
 — router {eq | neq} router-instance [regexp]
 — no router
 — severity {eq | neq | lt | lte | gt | gte} severity-level
 — no severity
 — subject {eq | neq} subject [regexp]
 — no subject

```

## Event Handling System (EHS) Commands

```

config
 — log
 — event-handling
 — [no] handler event-handler-name
 — action-list
 — [no] entry entry-id
 — description description-string
 — no description
 — [no] script-policy script-policy-name [owner owner-name]
 — no script-policy
 — description description-string
 — no description
 — [no] shutdown

```

## Event Trigger Commands

```

config
 — log
 — event-trigger
 — [no] event application-id event-name-id
 — description description-string
 — no description
 — [no] shutdown
 — [no] trigger-entry entry-id
 — event-handler event-handler-name
 — [no] event-handler
 — description description-string
 — no description
 — log-filter filter-id
 — [no] log-filter

```

## Log ID Commands

Refer to the 7x50 SR OS Services Guide for information about configuring logs in a VPRN service.

```

config
 — log
 — [no] log-id log-id
 — description description-string
 — no description
 — filter filter-id
 — no filter
 — from {[main] [security] [change] [debug-trace]}
 — no from
 — [no] shutdown
 — time-format {local | utc}
 — to console
 — to file log-file-id
 — to memory [size]
 — to session
 — to snmp [size]
 — to syslog syslog-id

```

## SNMP Trap Group Commands

Refer to the 7x50 SR OS Services Guide for information about configuring SNMP trap groups in a VPRN service.

```

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

Refer to the 7x50 SR OS Services Guide for information about configuring syslogs in a VPRN service.

```

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

Refer to the 7x50 SR OS Services Guide for information about log show routines for VPRN services.

**show**

— **log**

- **accounting-policy** [*acct-policy-id*] [**access** | **network**]
- **accounting-records**
- **applications**
- **event-control** [**application** [*event-name* | *event-number*]]
- **event-handling**
  - **handler** [*handler-name*]
  - **handler detail**
- **file-id** [*log-file-id*]
- **filter-id** [*filter-id*]
- **log-collector**
- **log-id** [*log-id*] [**severity** *severity-level*] [**application** *application*] [**sequence** *from-seq* [*to-seq*]] [**count** *count*] [**router** *router-instance*] [**expression**] [**subject** *subject* [**regexp**]] [**ascending|descending**] [**message format** [**msg-regexp**]]
- **snmp-trap-group** [*log-id*]
- **syslog** [*syslog-id*]

### Clear Command

**clear**

— **log** *log-id*

---

## Configuration Commands

---

### Generic Commands

#### description

<b>Syntax</b>	<b>description</b> <i>string</i> <b>no description</b>
<b>Context</b>	config>log>filter config>log>filter>entry config>log>log-id config>log>accounting-policy config>log>event-handling>handler config>log>event-handling>handler>action-list>entry config>log>event-trigger>event config>log>event-trigger>event>trigger-entry config>log>file-id config>log>syslog config>log>snmp-trap-group
<b>Description</b>	This command creates a text description stored in the configuration file for a configuration context. The <b>description</b> command associates a text string with a configuration context to help identify the content in the configuration file.  The <b>no</b> form of the command removes the string from the configuration.
<b>Default</b>	No text description is associated with this configuration. The string must be entered.
<b>Parameters</b>	<i>string</i> — The description can contain a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

#### shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>log>log-id config>log>accounting-policy config>log>event-handling>handler config>log>event-trigger>event
<b>Description</b>	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.

## app-route-notifications

**Syntax**     **app-route-notifications**

**Context**     config>log

**Description**     Specific system applications in SR OS can take action based on a route to certain IP destinations being available. This CLI branch contains configuration related to these route availability notifications. A delay can be configured between the time that a route is determined as available in the CPM, and the time that the application is notified of the available route. For example, this delay may be used to increase the chances that other system modules (such as IOMs/XCMs/MDAs/XMAs) are fully programmed with the new route before the application takes action. Currently, the only application that acts upon these *route available* or *route changed* notifications with their configurable delays is the SNMP replay feature, which receives notifications of route availability to the SNMP trap receiver destination IP address.

## cold-start-wait

**Syntax**     **[no] cold-start-wait**

**Context**     config>log>app-route-notifications

**Description**     The time delay that must pass before notifying specific CPM applications that a route is available after a cold reboot.

**Default**     no cold-start-wait

**Parameters**     — **Values**     seconds: 1 – 300

**Default**     0



## route-recovery-wait

<b>Syntax</b>	<b>[no] route-recovery-wait</b>	
<b>Context</b>	config>log>app-route-notifications	
<b>Description</b>	The time delay that must pass before notifying specific CPM applications after the recovery or change of a route during normal operation.	
<b>Default</b>	no route-recovery-wait	
<b>Parameters</b>	<b>— Values</b>	seconds: 1 – 100
	<b>Default</b>	0

## event-control

<b>Syntax</b>	<b>event-control</b> <i>application-id</i> [ <i>event-name</i>   <i>event-number</i> ] [ <b>generate</b> ][ <i>severity-level</i> ] [ <b>throttle</b> ] [ <b>specific-throttle-rate</b> <i>events-limit</i> <b>interval</b> <i>seconds</i>   <b>disable-specific-throttle</b> ] <b>event-control</b> <i>application-id</i> [ <i>event-name</i>   <i>event-number</i> ] <b>suppress</b> <b>no event-control</b> <i>application</i> [ <i>event-name</i>   <i>event-number</i> ]	
<b>Context</b>	config>log	
<b>Description</b>	<p>This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.</p> <p>Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation which directs it to be generated or suppressed.</p> <p>Events are generated with a default severity level that can be modified by using the <i>severity-level</i> option.</p> <p>Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are squelched. In reverse, indiscriminate application may cause excessive overhead.</p> <p>The rate of event generation can be throttled by using the <b>throttle</b> parameter.</p> <p>The <b>no</b> form of the command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, suppress, and throttle options will also be reset to the initial values.</p>	
<b>Default</b>	Each event has a set of default settings. To display a list of all events and the current configuration use the <b>event-control</b> 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. Some examples of valid applications are:
- application\_assurance, aps, bgp, chassis, debug, dhcp, efm\_oam, eth\_cfm, filter, gsmp, igmp\_snooping, ip, isis, lag, ldp, li, lldp, logger, mcpaht, mc\_redundancy, mirror, mld\_snooping, mpls, ntp, oam, ospf, pim\_snooping, port, ppp, 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.
- Default** generate
- specific-throttle-rate** *events-limit* — The log event throttling rate can be configured independently for each log event using this keyword. This specific-throttle-rate overrides the globally configured throttle rate (**configure>log>throttle-rate**) for the specific log event.
- Values** 1 — 20000
- interval** *seconds* — specifies the number of seconds that the specific throttling intervals lasts.
- Values** 1 — 1200
- disable-specific-throttle** — Specifies to disable the **specific-throttle-rate**.

## event-damping

<b>Syntax</b>	<b>[no] event-damping</b>
<b>Context</b>	config>log
<b>Description</b>	<p>This command allows the user to set the event damping algorithm to suppress QoS or filter change events.</p> <p>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 (<b>no event-damping</b>), it may take much longer for a large CLI configuration file to be processed when manually “exceed” after system bootup.</p>

## route-preference

<b>Syntax</b>	<b>route-preference primary {inband   outband} secondary {inband   outband   none}</b> <b>no route-preference</b>
<b>Context</b>	config>log
<b>Description</b>	<p>This command specifies the primary and secondary routing preference for traffic generated for SNMP notifications and syslog messages. If the remote destination is not reachable through the routing context specified by primary route preference then the secondary routing preference will be attempted.</p> <p>The <b>no</b> form of the command reverts to the default values.</p>
<b>Default</b>	no route-preference
<b>Parameters</b>	<p><b>primary</b> — Specifies the primary routing preference for traffic generated for SNMP notifications and syslog messages.</p> <p><b>Default</b> outband</p> <p><b>secondary</b> — Specifies the secondary routing preference for traffic generated for SNMP notifications and syslog messages. The routing context specified by the secondary route preference will be attempted if the remote destination was not reachable by the primary routing preference, specified by primary route preference. The value specified for the secondary routing preference must be distinct from the value for primary route preference.</p> <p><b>Default</b> inband</p> <p><b>inband</b> — Specifies that the logging utility will attempt to use the base routing context to send SNMP notifications and syslog messages to remote destinations.</p> <p><b>outband</b> — Specifies that the logging utility will attempt to use the management routing context to send SNMP notifications and syslog messages to remote destinations.</p> <p><b>none</b> — Specifies that no attempt will be made to send SNMP notifications and syslog messages to remote destinations.</p>

## Log File Commands

### file-id

<b>Syntax</b>	<b>[no] file-id</b> <i>file-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.</p> <p>This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the <b>to</b> command under <b>log-id</b> or <b>accounting-policy</b> to direct specific logging or billing source streams to the file destination.</p> <p>A file ID can only be assigned to either <i>one</i> <b>log-id</b> or <i>one</i> <b>accounting-policy</b>. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.</p> <p>A file is created when the file ID defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.</p> <p>The file names for a log are created by the system as summarized in the table below:</p>

File Type	File Name
Log File	<i>logllff-timestamp</i>
Accounting File	<i>actaaaff-timestamp</i>

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the *file-id*
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
  - *yyyy* is the year (for example, 2006)
  - *mm* is the month number (for example, 12 for December)
  - *dd* is the day of the month (for example, 03 for the 3rd of the month)
  - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
  - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
  - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a *gz* extension.

When initialized, each file will contain:

- The *log-id* description.
- The time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

<b>Default</b>	No default file IDs are defined.
<b>Parameters</b>	<i>file-id</i> — The file identification number for the file, expressed as a decimal integer.
<b>Values</b>	1 — 99

## location

<b>Syntax</b>	<b>location</b> <i>cflash-id</i> [ <i>backup-cflash-id</i> ] <b>no location</b>
<b>Context</b>	config>log>file <i>file-id</i>
<b>Description</b>	<p>This command specifies the primary and optional backup location where the log or billing file will be created.</p> <p>The <b>location</b> 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.).</p> <p>When multiple location commands are entered in a single file ID context, the last command overwrites the previous command.</p> <p>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 <b>clear log</b> <i>log-id</i> command is entered to manually rollover the log file.</p> <p>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.</p>

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.

<b>Default</b>	Log files are created on cf1: and accounting files are created on cf2:.
<b>Parameters</b>	<i>cflash-id</i> — Specify the primary location.
<b>Values</b>	cflash-id: cf1:, cf2:, cf3:
	<i>backup-cflash-id</i> — Specify the secondary location.
<b>Values</b>	cflash-id: cf1:, cf2:, cf3:

## rollover

<b>Syntax</b>	<b>rollover</b> <i>minutes</i> [ <b>retention</b> <i>hours</i> ] <b>no rollover</b>
<b>Context</b>	config>log>file <i>file-id</i>
<b>Description</b>	<p>This command configures how often an event or accounting log is rolled over or partitioned into a new file.</p> <p>An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the <b>rollover</b> time, expressed in minutes.</p> <p>The <b>retention</b> option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.</p> <p>When multiple <b>rollover</b> commands for a <i>file-id</i> are entered, the last command overwrites the previous command.</p>
<b>Default</b>	<b>rollover 1440 retention 12</b>
<b>Parameters</b>	<p><i>minutes</i> — The rollover time, in minutes.</p> <p><b>Values</b> 5 — 10080</p> <p><i>retention hours</i>. 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.</p> <p><b>Default</b> 12</p> <p><b>Values</b> 1 — 500</p>

## Log Filter Commands

### filter

<b>Syntax</b>	<b>[no] filter</b> <i>filter-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.</p> <p>Filters are configured in the <b>filter</b> <i>filter-id</i> context and then applied to a log in the <b>log-id</b> <i>log-id</i> context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.</p> <p>Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.</p> <p>The <b>no</b> form of the command removes the filter association from log IDs which causes those logs to forward all events.</p>
<b>Default</b>	No event filters are defined.
<b>Parameters</b>	<i>filter-id</i> — The filter ID uniquely identifies the filter.
<b>Values</b>	1 — 1000

### default-action

<b>Syntax</b>	<b>default-action {drop   forward}</b> <b>no default-action</b>
<b>Context</b>	config>log>filter <i>filter-id</i>
<b>Description</b>	<p>The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.</p> <p>When multiple <b>default-action</b> commands are entered, the last command overwrites the previous command.</p> <p>The <b>no</b> form of the command reverts the default action to the default value (forward).</p>
<b>Default</b>	<b>default-action forward</b> — The events which are not explicitly dropped by an event filter match are forwarded.
<b>Parameters</b>	<p><b>drop</b> — The events which are not explicitly forwarded by an event filter match are dropped.</p> <p><b>forward</b> — The events which are not explicitly dropped by an event filter match are forwarded.</p>

---

## Log Filter Entry Commands

### action

<b>Syntax</b>	
<b>Syntax</b>	<b>action</b> { <b>drop</b>   <b>forward</b> } <b>no action</b>
<b>Context</b>	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
<b>Description</b>	<p>This command specifies a drop or forward action associated with the filter entry. If neither <b>drop</b> nor <b>forward</b> is specified, the <b>default-action</b> will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.</p> <p>Multiple action statements entered will overwrite previous actions.</p> <p>The <b>no</b> form of the command removes the specified <b>action</b> statement.</p>
<b>Default</b>	Action specified by the <b>default-action</b> command will apply.
<b>Parameters</b>	<p><b>drop</b> — Specifies packets matching the entry criteria will be dropped.</p> <p><b>forward</b> — Specifies packets matching the entry criteria will be forwarded.</p>

### entry

<b>Syntax</b>	[ <b>no</b> ] <b>entry</b> <i>entry-id</i>
<b>Context</b>	config>log>filter <i>filter-id</i>
<b>Description</b>	<p>This command is used to create or edit an event filter entry. Multiple entries may be created using unique <i>entry-id</i> numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.</p> <p>Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.</p> <p>The <b>no</b> form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.</p>
<b>Default</b>	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

<b>Syntax</b>	<b>[no] match</b>
<b>Context</b>	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
<b>Description</b>	<p>This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.</p> <p>If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.</p> <p>Use the <b>application</b> command to display a list of the valid applications.</p> <p>Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple <b>match</b> statements cannot be entered per entry.</p> <p>The <b>no</b> form of the command removes the match criteria for the <i>entry-id</i>.</p>
<b>Default</b>	No match context is defined.

### application

<b>Syntax</b>	<b>application {eq   neq} application-id</b> <b>no application</b>
<b>Context</b>	config>log>filter <i>filter-id</i> >entry <i>entry-id</i> >match
<b>Description</b>	<p>This command adds an OS application as an event filter match criterion.</p> <p>An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES etc. Only one application can be specified. The latest <b>application</b> command overwrites the previous command.</p> <p>The <b>no</b> form of the command removes the application as a match criterion.</p>
<b>Default</b>	<b>no application</b> — No application match criterion is specified.
<b>Parameters</b>	<b>eq   neq</b> — 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** application\_assurance, aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, diameter, dynsvc, efm\_oam, elmi, ering, eth\_cfm, etun, fiter, gsmpp, igh, igmp,

igmp\_snooping, ip, ipsec, isis, l2tp, lag, ldp, li, lldp, logger, mcpath, mc\_redundancy, mirror, mld, mld\_snooping, mpls, mpls\_tp, msdp, nat, ntp, oam, open\_flow, ospf, pim, pim\_snooping, port, ppp, pppoe, ptp, radius, rip, rip\_ng, route\_policy, rsvp, security, snmp, stp, svcmgr, system, user, video, vrrp, vrtr, wlan\_gw, wpp

## message

<b>Syntax</b>	<b>message {eq   neq} pattern pattern [regex]</b> <b>no message</b>
<b>Context</b>	config>log>filter>entry>match
<b>Description</b>	This command adds system messages as a match criterion. The <b>no</b> form of the command removes messages as a match criterion.
<b>Parameters</b>	<b>eq</b> — Determines if the matching criteria should be equal to the specified value. <b>neq</b> — Determines if the matching criteria should not be equal to the specified value. <b>pattern pattern</b> — Specifies a message up to 400 characters to be used in the match criteria. <b>regex</b> — Specifies the type of string comparison to use to determine if the log event matches the value of <b>message</b> command parameters. When the <b>regex</b> keyword is not specified, the default matching algorithm used is a basic substring match.

## number

<b>Syntax</b>	<b>number {eq   neq   lt   lte   gt   gte} event-id</b> <b>no number</b>
<b>Context</b>	config>log>filter <i>filter-id</i> >entry <i>entry-id</i> >match
<b>Description</b>	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 <b>number</b> command can be entered per event filter entry. The latest <b>number</b> command overwrites the previous command. The <b>no</b> form of the command removes the event number as a match criterion.
<b>Default</b>	<b>no event-number</b> — No event ID match criterion is specified.
<b>Parameters</b>	<b>eq   neq   lt   lte   gt   gte</b> — 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

Operator	Notes
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

<b>Syntax</b>	<b>router {eq   neq} router-instance [regex]</b> <b>no router</b>
<b>Context</b>	config>log>filter>entry>match
<b>Description</b>	This command specifies the log event matches for the router.
<b>Parameters</b>	<p><b>eq</b> — Determines if the matching criteria should be equal to the specified value.</p> <p><b>neq</b> — Determines if the matching criteria should not be equal to the specified value.</p> <p><i>router-instance</i> — Specifies a router name up to 32 characters to be used in the match criteria.</p> <p><b>regex</b> — Specifies the type of string comparison to use to determine if the log event matches the value of <b>router</b> command parameters. When the <b>regex</b> keyword is specified, the string in the <b>router</b> command is a regular expression string that will be matched against the subject string in the log event being filtered.</p>

## severity

<b>Syntax</b>	<b>severity {eq   neq   lt   lte   gt   gte} severity-level</b> <b>no severity</b>
<b>Context</b>	config>log>filter>entry>match
<b>Description</b>	<p>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.</p> <p>The <b>no</b> form of the command removes the severity match criterion.</p>
<b>Default</b>	<b>no severity</b> — 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 [regex]**  
**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 the **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

---

## Event Handling System (EHS) Commands

### event-handling

<b>Syntax</b>	<b>event-handling</b>
<b>Context</b>	config>log
<b>Description</b>	This command enables the context to configure event handling within the Event Handler System (EHS).

### handler

<b>Syntax</b>	<b>[no] handler</b> <i>event-handler-name</i>
<b>Context</b>	config>log>event-handling
<b>Description</b>	This command configures an EHS handler. The <b>no</b> form of the command removes the specified EHS handler.
<b>Parameters</b>	<i>event-handler-name</i> — Specifies the name of the EHS handler. Can be up to 32 characters maximum.

### action-list

<b>Syntax</b>	<b>action-list</b>
<b>Context</b>	config>log>event-handling>handler
<b>Description</b>	This command enables the context to configure the EHS handler action list.

### entry

<b>Syntax</b>	<b>[no] entry</b> <i>entry-id</i>
<b>Context</b>	config>log>event-handling>handler>action-list
<b>Description</b>	This command configures an EHS handler action-list entry. A handler can have multiple actions where each action, for example, could request the execution of a different script. When the handler is triggered it will walk through the list of configured actions. The <b>no</b> form of the command removes the specified EHS handler action-list entry.
<b>Parameters</b>	<i>entry-id</i> — Specifies the identifier of the EHS handler entry.
<b>Values</b>	1 — 1500

### script-policy

<b>Syntax</b>	<b>script-policy</b> <i>policy-name</i> [ <b>owner</b> <i>policy-owner</i> ] <b>no script-policy</b>
<b>Context</b>	config>log>event-handling>handler>action-list>entry
<b>Description</b>	This command configures the script policy parameters to use for this EHS handler action-list entry. The associated script is launched when the handler is triggered.
<b>Parameters</b>	<i>policy-name</i> — Specifies the script policy name. Can be up to 32 characters maximum. <b>owner</b> <i>policy-owner</i> — Specifies the script policy owner. Can be up to 32 characters maximum.
<b>Default</b>	“TiMOS CLI”



## Event Trigger Commands

### event-trigger

<b>Syntax</b>	<b>event-trigger</b>
<b>Context</b>	config>log
<b>Description</b>	This command enables the context to configure log events as triggers for Event Handling System (EHS) handlers.

### event

<b>Syntax</b>	<b>[no] event</b> <i>application-id</i> <i>event-name-id</i>
<b>Context</b>	config>log>event-trigger
<b>Description</b>	<p>This command configures a specific log event as a trigger for one or more EHS handlers. Further matching criteria can be applied to only trigger certain handlers with certain instances of the log event.</p> <p>The <b>no</b> form of the command removes the specified trigger event.</p>
<b>Parameters</b>	<p><i>application-id</i> — Specifies the type of application that triggers the event.</p> <p><b>Values</b> application_assurance   aps   atm   bgp   calltrace   cflowd   chassis   debug   dhcp   dhcps   diameter   dynsvc   efm_oam   elmi   ering   eth_cfm   etun   filter   gsmp   gmpls   igh   igmp   igmp_snooping   ip   ipsec   isis   l2tp   lag   ldp   li   lldp   lmp   logger   mcpath   mc_redundancy   mirror   mld   mld_snooping   mpls   mpls_tp   msdp   nat   ntp   oam   open_flow   ospf   pim   pim_snooping   port   ppp   pppoe   radius   rip   rip_ng   route_policy   rsvp   security   snmp   stp   svcmgr   system   user   video   vrrp   vrtr   wlan_gw   wpp</p> <p><i>event-name-id</i> — Specifies the name or numerical identifier of the event.</p> <p><b>Values</b> 0 — 4294967295   <i>event-name</i>: 32 characters max</p>

### trigger-entry

<b>Syntax</b>	<b>[no] trigger-entry</b> <i>entry-id</i>
<b>Context</b>	config>log>event-trigger>event
<b>Description</b>	<p>This command configures an instance of a trigger for an EHS handler. A trigger entry binds a set of matching criteria for a log event to a particular handler. If the log event occurs in the system and matches the criteria configured in the associated log filter then the handler will be executed.</p> <p>The <b>no</b> form of the command removes the specified trigger entry.</p>

**Parameters**    *entry-id* — Specifies the identifier of the EHS event trigger entry.  
**Values**        1 — 1500

### event-handler

**Syntax**        **event-handler** *event-handler*  
                 **no event-handler**

**Context**        config>log>event-trigger>event>trigger-entry

**Description**    This command configures the event handler to be used for this trigger entry.

**Parameters**    *event-handler* — Specifies the name of the event handler. Can be up to 32 characters maximum.

### log-filter

**Syntax**        **log-filter** *filter-id*  
                 **no log-filter**

**Context**        config>log>event-trigger>event>trigger-entry

**Description**    This command configures the log filter to be used for this trigger entry. The log filter defines the matching criteria that must be met in order for the log event to trigger the handler execution. The log filter is applied to the log event and, if the filtering decision results in a ‘forward’ action, then the handler is triggered.

                 It is typically unnecessary to configure match criteria for ‘application’ or ‘number’ in the log filter used for EHS since the particular filter is only applied for a specific log event application and number, as configured under **config>log>event-trigger**.

**Parameters**    *filter-id* — Specifies the identifier of the filter.  
**Values**        1 — 1500

## Syslog Commands

### syslog

<b>Syntax</b>	<b>[no] syslog</b> <i>syslog-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.</p> <p>A valid <i>syslog-id</i> must have the target syslog host address configured.</p> <p>A maximum of 10 syslog-id's can be configured.</p> <p>No log events are sent to a syslog target address until the syslog-id has been configured as the log destination (<b>to</b>) in the log-id node.</p> <p>The syslog ID configured in the <b>configure/service/vprn</b> context has a local VPRN scope and only needs to be unique within the specific VPRN instance. The same ID can be reused under a different VPRN service or in the global log context under <b>config&gt;log</b>.</p>
<b>Default</b>	No syslog IDs are defined.
<b>Parameters</b>	<p><i>syslog-id</i> — The syslog ID number for the syslog destination, expressed as a decimal integer.</p> <p><b>Values</b>      1 — 10</p>

### address

<b>Syntax</b>	<b>address</b> <i>ip-address</i> <b>no address</b>
<b>Context</b>	config>log>syslog <i>syslog-id</i>
<b>Description</b>	<p>This command adds the syslog target host IP address to/from a syslog ID.</p> <p>This parameter is mandatory. If no <b>address</b> is configured, syslog data cannot be forwarded to the syslog target host.</p> <p>Only one address can be associated with a <i>syslog-id</i>. If multiple addresses are entered, the last address entered overwrites the previous address.</p> <p>The same syslog target host can be used by multiple log IDs.</p> <p>The <b>no</b> form of the command removes the syslog target host IP address.</p>
<b>Default</b>	<b>no address</b> — There is no syslog target host IP address defined for the syslog ID.
<b>Parameters</b>	<i>ip-address</i> — The IP address of the syslog target host in dotted decimal notation.

## facility

<b>Syntax</b>	<b>facility</b> <i>syslog-facility</i> <b>no facility</b>
<b>Context</b>	config>log>syslog <i>syslog-id</i>
<b>Description</b>	<p>This command configures the facility code for messages sent to the syslog target host.</p> <p>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 <i>facility-code</i> entered overwrites the previous facility-code.</p> <p>If multiple facilities need to be generated for a single syslog target host, then multiple <b>log-id</b> 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.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>
<b>Default</b>	<b>local7</b> — syslog entries are sent with the local7 facility code.
<b>Parameters</b>	<p><i>syslog-facility</i> — 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.</p> <p><b>Values</b>      kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7</p>

Valid responses per RFC3164, *The BSD syslog Protocol*, are listed in the table below.

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news
8	uucp
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0

Numerical Code	Facility Code
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7
<b>Values</b>	0 — 23

## log-prefix

<b>Syntax</b>	<b>log-prefix</b> <i>log-prefix-string</i> <b>no log-prefix</b>
<b>Context</b>	config>log>syslog <i>syslog-id</i>
<b>Description</b>	<p>This command adds the string prepended to every syslog message sent to the syslog host.</p> <p>RFC3164, <i>The BSD syslog Protocol</i>, allows a alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.</p> <p>Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.</p> <p>The <b>no</b> form of the command removes the log prefix string.</p>
<b>Default</b>	<b>no log-prefix</b> — no prepend log prefix string defined.
<b>Parameters</b>	<i>log-prefix-string</i> — An alphanumeric string of up to 32 characters. Spaces and colons ( : ) cannot be used in the string.

## level

<b>Syntax</b>	<b>level</b> <i>syslog-level</i> <b>no level</b>
<b>Context</b>	config>log>syslog <i>syslog-id</i>
<b>Description</b>	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

Router 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

<b>Syntax</b>	<b>throttle-rate</b> <i>events</i> [ <b>interval</b> <i>seconds</i> ] <b>no throttle-rate</b>
<b>Context</b>	config>log
<b>Description</b>	This command configures an event throttling rate.
<b>Parameters</b>	<p><i>events</i> — Specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, for example, the event drop count will be incremented. At the end of the throttle interval if any events have been dropped a trap notification will be sent.</p> <p><b>Values</b>      1 — 20000</p> <p><b>Default</b>     2000</p> <p><b>interval</b> <i>seconds</i> — Specifies the number of seconds that an event throttling interval lasts.</p> <p><b>Values</b>      1 — 1200</p> <p><b>Default</b>     1</p>

---

## SNMP Trap Groups

### snmp-trap-group

<b>Syntax</b>	<b>[no] snmp-trap-group</b> <i>log-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.</p> <p>A group specifies the types of SNMP traps and specifies the log ID which will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.</p> <p>To suppress the generation of all alarms and traps see the <b>event-control</b> command. To suppress alarms and traps that are sent to this log-id, see the <b>filter</b> command. Once alarms and traps are generated they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.</p> <p>The <b>no</b> form of the command deletes the SNMP trap group.</p>
<b>Default</b>	There are no default SNMP trap groups.
<b>Parameters</b>	<p><i>log-id</i> — The log ID value of a log configured in the <b>log-id</b> context. Alarms and traps cannot be sent to the trap receivers until a valid <i>log-id</i> exists.</p> <p><b>Values</b>      1 — 99</p>

### trap-target

<b>Syntax</b>	<b>trap-target</b> <i>name</i> [ <b>address</b> <i>ip-address</i> ] [ <b>port</b> <i>port</i> ] [ <b>snmpv1</b>   <b>snmpv2c</b>   <b>snmpv3</b> ] <b>notify-community</b> <i>communityName</i>   <i>snmpv3SecurityName</i> [ <b>security-level</b> { <b>no-auth-no-privacy</b>   <b>auth-no-privacy</b>   <b>privacy</b> }] [ <b>replay</b> ] <b>no trap-target</b> <i>name</i>
<b>Context</b>	config>log>snmp-trap-group
<b>Description</b>	<p>This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.</p> <p>Before an SNMP trap can be issued to a trap receiver, the <b>log-id</b>, <b>snmp-trap-group</b> and at least one <b>trap-target</b> must be configured.</p> <p>The <b>trap-target</b> command is used to add/remove a trap receiver from an <b>snmp-trap-group</b>. The operational parameters specified in the command include:</p> <ul style="list-style-type: none"> <li>• The IP address of the trap receiver</li> <li>• The UDP port used to send the SNMP trap</li> <li>• SNMP version</li> </ul>



- 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** parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each router 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)

**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. The cold-start-wait and route-recovery-wait timers under `config>log>app-route-notifications` can help reduce the probability of lost events.

## filter

<b>Syntax</b>	<b>filter</b> <i>filter-id</i> <b>no filter</b>
<b>Context</b>	config>log>log-id <i>log-id</i>
<b>Description</b>	<p>This command adds an event filter policy with the log destination.</p> <p>The <b>filter</b> command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.</p> <p>An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination <b>snmp-trap-group</b>.</p> <p>The application of filters for debug messages is limited to application and subject only.</p> <p>Accounting records cannot be filtered using the <b>filter</b> command.</p> <p>Only one filter-id can be configured per log destination.</p> <p>The <b>no</b> form of the command removes the specified event filter from the <i>log-id</i>.</p>
<b>Default</b>	<b>no filter</b> — No event filter policy is specified for a <i>log-id</i> .
<b>Parameters</b>	<i>filter-id</i> . The event filter policy ID is used to associate the filter with the <i>log-id</i> configuration. The event filter policy ID must already be defined in <b>config&gt;log&gt;filter</b> <i>filter-id</i> .
<b>Values</b>	1 — 1000

## from

<b>Syntax</b>	<b>from</b> {[ <b>main</b> ] [ <b>security</b> ] [ <b>change</b> ] [ <b>debug-trace</b> ]} <b>no from</b>
<b>Context</b>	config>log>log-id <i>log-id</i>
<b>Description</b>	<p>This command selects the source stream to be sent to a log destination.</p> <p>One or more source streams must be specified. The source of the data stream must be identified using the <b>from</b> command before you can configure the destination using the <b>to</b> command. The <b>from</b> command can identify multiple source streams in a single statement (for example: <b>from main change debug-trace</b>).</p> <p>Only one <b>from</b> command may be entered for a single <i>log-id</i>. If multiple <b>from</b> commands are configured, then the last command entered overwrites the previous <b>from</b> command.</p> <p>The <b>no</b> form of the command removes all previously configured source streams.</p>
<b>Default</b>	No source stream is configured.
<b>Parameters</b>	<b>main</b> — Instructs all events in the main event stream to be sent to the destination defined in the <b>to</b> command for this destination <i>log-id</i> . The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the <b>filter</b> 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

<b>Syntax</b>	<b>[no] log-id</b> <i>log-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates a context to configure destinations for event streams.</p> <p>The <b>log-id</b> context is used to direct events, alarms/traps, and debug information to respective destinations.</p> <p>A maximum of 10 logs can be configured.</p> <p>Before an event can be associated with this log-id, the <b>from</b> command identifying the source of the event must be configured.</p> <p>Only one destination can be specified for a <i>log-id</i>. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.</p> <p>Use the <b>event-control</b> command to suppress the generation of events, alarms, and traps for all log destinations.</p> <p>An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.</p> <p>Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages. Log-ID 100 captures log messages with a severity level of major and above.</p> <p>Note that Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.</p> <p>The <b>no</b> form of the command deletes the log destination ID from the configuration.</p>
<b>Default</b>	No log destinations are defined.
<b>Parameters</b>	<p><i>log-id</i> — The log ID number, expressed as a decimal integer.</p> <p><b>Values</b>      1 — 100</p>

## to console

<b>Syntax</b>	<b>to console</b>
<b>Context</b>	config>log>log-id <i>log-id</i>
<b>Description</b>	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all the entries are dropped.</p> <p>The source of the data stream must be specified in the <b>from</b> command prior to configuring the destination with the <b>to</b> command.</p> <p>The <b>to</b> command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
<b>Default</b>	No destination is specified.

## to file

<b>Syntax</b>	<b>to file</b> <i>log-file-id</i>
<b>Context</b>	config>log>log-id <i>log-id</i>
<b>Description</b>	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a specified file.</p> <p>The source of the data stream must be specified in the <b>from</b> command prior to configuring the destination with the <b>to</b> command.</p> <p>The <b>to</b> command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
<b>Default</b>	No destination is specified.
<b>Parameters</b>	<p><i>log-file-id</i> — Instructs the events selected for the log ID to be directed to the <i>log-file-id</i>. The characteristics of the <i>log-file-id</i> referenced here must have already been defined in the <b>config&gt;log&gt;file</b> <i>log-file-id</i> context.</p> <p><b>Values</b>      1 — 99</p>

## to memory

<b>Syntax</b>	<b>to memory</b> [ <i>size</i> ]
<b>Context</b>	config>log>log-id <i>log-id</i>
<b>Description</b>	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a memory log.</p>

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 “to session” configuration is removed. A log ID with a *session* destination is saved in the configuration file but the “to session” part is not stored.

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.

<b>Default</b>	none
<b>Parameters</b>	<i>size</i> — The <i>size</i> parameter defines the number of events stored in this memory log.
<b>Default</b>	100
<b>Values</b>	50 — 1024

## to syslog

<b>Syntax</b>	<b>to syslog</b> <i>syslog-id</i>
<b>Context</b>	config>log>log-id
<b>Description</b>	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1k bytes.</p> <p>The source of the data stream must be specified in the <b>from</b> command prior to configuring the destination with the <b>to</b> command.</p> <p>The <b>to</b> command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.</p>
<b>Default</b>	none
<b>Parameters</b>	<p><i>syslog-id</i> — Instructs the events selected for the log ID to be directed to the <i>syslog-id</i>. The characteristics of the <i>syslog-id</i> referenced here must have been defined in the <b>config&gt;log&gt;syslog</b> <i>syslog-id</i> context.</p> <p><b>Values</b> 1 — 10</p>

## time-format

<b>Syntax</b>	<b>time-format</b> { <i>local</i>   <i>utc</i> }
<b>Context</b>	config>log>log-id
<b>Description</b>	This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.
<b>Default</b>	utc
<b>Parameters</b>	<p><b>local</b> — Specifies that timestamps are written in the system's local time.</p> <p><b>utc</b> — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.</p>

---

## Accounting Policy Commands

### accounting-policy

<b>Syntax</b>	<b>accounting-policy</b> <i>policy-id</i> [ <i>interval minutes</i> ] <b>no accounting-policy</b> <i>policy-id</i>
<b>Context</b>	config>log
<b>Description</b>	<p>This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.</p> <p>Access accounting policies are policies that can be applied to one or more SAPs. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.</p> <p>If an accounting policy is not specified on a SAP, then accounting records are produced in accordance with the access policy designated as the <b>default</b>. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.</p> <p>Only one policy can be regarded as the default access policy. If a policy is configured as the default policy, then a <b>no default</b> 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.</p> <p>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.</p> <p>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 <b>default</b> command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.</p> <p>Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a <b>no default</b> 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.</p> <p>The <b>no</b> form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.</p>
<b>Default</b>	No default accounting policy is defined.
<b>Parameters</b>	<i>policy-id</i> — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.
<b>Values</b>	1 — 99



## collection-interval

<b>Syntax</b>	<b>collection-interval</b> <i>minutes</i> <b>no collection-interval</b>
<b>Context</b>	config>log>acct-policy
<b>Description</b>	This command configures the accounting collection interval.
<b>Parameters</b>	<i>minutes</i> — Specifies the interval between collections, in minutes.
<b>Values</b>	1 — 120 A range of 1 — 4 is only allowed when the record type is set to SAA.

## auto-bandwidth

<b>Syntax</b>	<b>[no] auto-bandwidth</b>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	In the configuration of an accounting policy this designates the accounting policy as the one used for auto-bandwidth statistics collection.
<b>Default</b>	no auto-bandwidth

## default

<b>Syntax</b>	<b>[no] default</b>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	<p>This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The record name must be specified prior to assigning an accounting policy as default.</p> <p>If a policy is configured as the default policy, then a <b>no default</b> command must be issued before a new default policy can be configured.</p>

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.

### include-router-info

<b>Syntax</b>	<b>[no] include-router-info</b>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	<p>This command allows operator to optionally include router information at the top of each accounting file generated for a given accounting policy.</p> <p>When the no version of this command is selected, optional router information is not include at the top of the file.</p>
<b>Default</b>	no include-router-info

### include-system-info

<b>Syntax</b>	<b>[no] include-system-info</b>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	<p>This command allows the operator to optionally include router information at the top of each accounting file generated for a given accounting policy.</p> <p>When the <b>no</b> version of this command is selected, optional router information is not include at the top of the file.</p>
<b>Default</b>	no include-router-info

## 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.

**NOTE:** aa, video and subscriber records are not applicable to the 7950 XRS.

```
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
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
33 complete-pm 5
34 video 10
35 kpi-system 5
36 kpi-bearer-mgmt 5
37 kpi-bearer-traffic 5
38 kpi-ref-point 5
39 kpi-path-mgmt 5
40 kci-iom-3 5
41 kci-system 5
42 kci-bearer-mgmt 5
```

```

43 kci-path-mgmt 5
44 complete-kpi 5
45 complete-kci 5
46 kpi-bearer-group 5
47 kpi-ref-path-group 5
48 kpi-kci-bearer-mgmt 5
49 kpi-kci-path-mgmt 5
50 kpi-kci-system 5
51 complete-kpi-kci 5
52 aa-performance 15
53 complete-ethernet-port 15
54 extended-service-ingress-egress 5
55 complete-network-ing-egr 15
56 aa-partition 15
57 complete-pm 5
0 unknown-record-name 0
59 kpi-bearer-traffic-gtp-endpoint 5
60 kpi-ip-reas 5
61 kpi-radius-group 5
62 kpi-ref-pt-failure-cause-code 5
63 kpi-dhcp-group 5
 complete-pm 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
2	service-egress-octets	5

Record Type	Accounting Record Name	Default Interval
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
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

Record Type	Accounting Record Name	Default Interval
32	saa	5
33	complete-pm	5
34	video	10
35	kpi-system	5
36	kpi-bearer-mgmt	5
37	kpi-bearer-traffic	5
38	kpi-ref-point	5
39	kpi-path-mgmt	5
40	kpi-iom-3	5
41	kci-system	5
42	kci-bearer-mgmt	5
43	kci-path-mgmt	5
44	complete-kpi	5
45	complete-kci	5
46	kpi-bearer-group	5
47	kpi-ref-path-group	5
48	kpi-kci-bearer-mgmt	5
49	kpi-kci-path-mgmt	5
50	kpi-kci-system	5
51	complete-kpi-kci	5
52	aa-performance	15
53	complete-ethernet-port	15
54	extended-service-ingress-egress	5
55	complete-network-ing-egr	15

to

<b>Syntax</b>	<b>to file</b> <i>file-id</i>
<b>Context</b>	config>log>accounting-policy <i>policy-id</i> This command specifies the destination for the accounting records selected for the accounting policy.
<b>Default</b>	No destination is specified.
<b>Parameters</b>	<p><i>file-id</i> — The <i>file-id</i> option specifies the destination for the accounting records selected for this destination. The characteristics of the file-id must have already been defined in the config&gt;log&gt;file context. A file-id can only be used once.</p> <p>The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.</p> <p>If the <b>to</b> command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.</p>
<b>Values</b>	1 — 99

---

## Accounting Policy Custom Record Commands

### collection-interval

<b>Syntax</b>	<b>collection-interval</b> <i>minutes</i> <b>no collection-interval</b>
<b>Context</b>	config>log>acct-policy
<b>Description</b>	This command configures the accounting collection interval. The <b>no</b> form of the command returns the value to the default.
<b>Default</b>	60
<b>Parameters</b>	<i>minutes</i> — Specifies the collection interval in minutes. <b>Values</b> 5 — 120

### custom-record

<b>Syntax</b>	<b>[no] custom-record</b>
<b>Context</b>	config>log>acct-policy
<b>Description</b>	This command enables the context to configure the layout and setting for a custom accounting record associated with this accounting policy. The <b>no</b> form of the command reverts the configured values to the defaults.

### aa-specific

<b>Syntax</b>	<b>[no] aa-specific</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	This command enables the context to configure information for this custom record. The <b>no</b> form of the command



## aa-sub-counters

<b>Syntax</b>	<b>aa-sub-counters [all]</b> <b>no aa-sub-counters</b>
<b>Context</b>	config>log>acct-policy>cr>aa
<b>Description</b>	This command enables the context to configure subscriber counter information. The <b>no</b> form of the command
<b>Parameters</b>	<b>all</b> — Specifies all counters.

## long-duration-flow-count

<b>Syntax</b>	<b>long-duration-flow-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	This command includes the long duration flow count. The <b>no</b> form of the command excludes the long duration flow count in the AA subscriber's custom record.
<b>Default</b>	no long-duration-flow-count

## medium-duration-flow-count

<b>Syntax</b>	<b>[no] medium-duration-flow-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	This command includes the medium duration flow count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the medium duration flow count.
<b>Default</b>	no medium-duration-flow-count

## short-duration-flow-count

<b>Syntax</b>	<b>[no] short-duration-flow-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	This command includes the short duration flow count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the short duration flow count.
<b>Default</b>	no short-duration-flow-count

## total-flow-duration

<b>Syntax</b>	<b>[no] total-flow-duration</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	This command includes the total flow duration flow count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the total flow duration flow count.

## total-flows-completed-count

<b>Syntax</b>	<b>[no] total-flows-completed-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	This command includes the total flows completed count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the total flow duration flow count.

## from-aa-sub-counters

<b>Syntax</b>	<b>[no] from-aa-sub-counters</b>
<b>Context</b>	config>log>acct-policy>cr>aa
<b>Description</b>	This command enables the context to configure Application Assurance “from subscriber” counter parameters. The <b>no</b> form of the command excludes the “from subscriber” count.

## all

<b>Syntax</b>	<b>all</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Default</b>	This command include all counters.

## flows-active-count

<b>Syntax</b>	<b>[no] flows-active-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the active flow count.  The <b>no</b> form of the command excludes the active flow count in the AA subscriber's custom record.
<b>Default</b>	no flows-active-count

## flows-admitted-count

<b>Syntax</b>	<b>[no] flows-admitted-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the admitted flow count.  The <b>no</b> form of the command excludes the flow's admitted count in the AA subscriber's custom record.
<b>Default</b>	no flows-admitted-count

## flows-denied-count

<b>Syntax</b>	<b>[no] flows-denied-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the flow's denied count in the AA subscriber's custom record.  The <b>no</b> form of the command excludes the flow's denied count.
<b>Default</b>	no flows-denied-count

## forwarding-class

<b>Syntax</b>	<b>[no] forwarding-class</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command enables the collection of a Forwarding Class bitmap information added to the XML aa-sub and router level accounting records.

**Default** no forwarding-class

### 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

<b>Syntax</b>	<b>[no] octets-denied-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the denied octet count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the denied octet count.
<b>Default</b>	no octets-denied-count

## packets-admitted-count

<b>Syntax</b>	<b>[no] packets-admitted-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the admitted packet count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the admitted packet count.
<b>Default</b>	no packets-admitted-count

## packets-denied-count

<b>Syntax</b>	<b>[no] packets-denied-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-from-sub-cntr config>log>acct-policy>cr>aa>aa-to-sub-cntr
<b>Description</b>	This command includes the denied packet count in the AA subscriber's custom record. The <b>no</b> form of the command excludes the denied packet count.
<b>Default</b>	no packets-denied-count

## to-aa-sub-counters

<b>Syntax</b>	<b>to-aa-sub-counters</b> <b>no to-aa-sub-counters</b>
<b>Context</b>	config>log>acct-policy>cr>aa
<b>Description</b>	This command enables the context to configure Application Assurance “to subscriber” counter parameters. The <b>no</b> form of the command excludes the “to subscriber” count.

## override-counter

<b>Syntax</b>	<b>[no] override-counter</b> <i>override-counter-id</i>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	This command enables the context to configure override counter (HSMDA) parameters. The <b>no</b> form of the command removes the ID from the configuration.
<b>Parameters</b>	<i>override-counter-id</i> — Specifies the override counter ID.
<b>Values</b>	1 — 8

## queue

<b>Syntax</b>	<b>[no] queue</b> <i>queue-id</i>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	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 <b>no</b> form of the command reverts to the default value.
<b>Parameters</b>	<i>queue-id</i> — Specifies the queue-id for which counters will be collected in this custom record.

## e-counters

<b>Syntax</b>	<b>[no] e-counters</b>
<b>Context</b>	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
<b>Description</b>	This command configures egress counter parameters for this custom record. The <b>no</b> form of the command reverts to the default value.

## i-counters

<b>Syntax</b>	<b>i-counters [all]</b> <b>no i-counters</b>
<b>Context</b>	config>log>acct-policy>cr>override-cntr config>log>acct-policy>cr>ref-override-cntr config>log>acct-policy>cr>ref-queue
<b>Description</b>	This command configures ingress counter parameters for this custom record. The <b>no</b> form of the command
<b>Parameters</b>	<b>all</b> — Specifies all ingress counters should be included.

## in-profile-octets-discarded-count

<b>Syntax</b>	<b>[no] in-profile-octets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in-profile octets discarded count. The <b>no</b> form of the command excludes the in-profile octets discarded count.

## in-profile-octets-forwarded-count

<b>Syntax</b>	<b>[no] in-profile-octets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in-profile octets forwarded count. The <b>no</b> form of the command excludes the in-profile octets forwarded count.

## in-profile-packets-discarded-count

<b>Syntax</b>	<b>[no] in-profile-packets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in-profile packets discarded count. The <b>no</b> form of the command excludes the in-profile packets discarded count.

## in-profile-packets-forwarded-count

<b>Syntax</b>	<b>[no] in-profile-packets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in-profile packets forwarded count. The <b>no</b> form of the command excludes the in-profile packets forwarded count.

## out-profile-octets-discarded-count

<b>Syntax</b>	<b>[no] out-profile-octets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile packets discarded count. The <b>no</b> form of the command excludes the out of profile packets discarded count.



## out-profile-octets-forwarded-count

<b>Syntax</b>	<b>[no] out-profile-octets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile octets forwarded count. The <b>no</b> form of the command excludes the out of profile octets forwarded count.

## out-profile-packets-discarded-count

<b>Syntax</b>	<b>[no] out-profile-packets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile packets discarded count. The <b>no</b> form of the command excludes the out of profile packets discarded count.

## out-profile-packets-forwarded-count

<b>Syntax</b>	<b>[no] out-profile-packets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile packets forwarded count. The <b>no</b> form of the command excludes the out of profile packets forwarded count.

## all-octets-offered-count

<b>Syntax</b>	<b>[no] all-octets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes all octets offered in the count. The <b>no</b> form of the command excludes the octets offered in the count.
<b>Default</b>	no all-octets-offered-count

## all-packets-offered-count

<b>Syntax</b>	<b>[no] all-packets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes all packets offered in the count. The <b>no</b> form of the command excludes the packets offered in the count.
<b>Default</b>	no all-packets-offered-count

## high-octets-discarded-count

<b>Syntax</b>	<b>[no] high-octets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the high octets discarded count. The <b>no</b> form of the command excludes the high octets discarded count.
<b>Default</b>	no high-octets-discarded-count

## high-octets-offered-count

<b>Syntax</b>	<b>[no] high-octets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the high octets offered count. The <b>no</b> form of the command excludes the high octets offered count.

## high-packets-discarded-count

<b>Syntax</b>	<b>[no] high-packets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the high packets discarded count. The <b>no</b> form of the command excludes the high packets discarded count.
<b>Default</b>	no high-packets-discarded-count

## high-packets-offered-count

<b>Syntax</b>	<b>[no] high-packets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the high packets offered count. The <b>no</b> form of the command excludes the high packets offered count.
<b>Default</b>	no high-packets-offered -count

## in-profile-octets-forwarded-count

<b>Syntax</b>	<b>[no] in-profile-octets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in profile octets forwarded count. The <b>no</b> form of the command excludes the in profile octets forwarded count.
<b>Default</b>	no in-profile-octets-forwarded-count

## in-profile-packets-forwarded-count

<b>Syntax</b>	<b>[no] in-profile-packets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the in profile packets forwarded count. The <b>no</b> form of the command excludes the in profile packets forwarded count.
<b>Default</b>	no in-profile-packets-forwarded-count

## low-octets-discarded-count

<b>Syntax</b>	<b>[no] low-octets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the low octets discarded count. The <b>no</b> form of the command excludes the low octets discarded count.
<b>Default</b>	no low-octets-discarded-count

## low-packets-discarded-count

<b>Syntax</b>	<b>[no] low-packets-discarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the low packets discarded count. The <b>no</b> form of the command excludes the low packets discarded count.
<b>Default</b>	no low-packets-discarded-count

## low-octets-offered-count

<b>Syntax</b>	<b>[no] low-octets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the low octets discarded count. The <b>no</b> form of the command excludes the low octets discarded count.

## low-packets-offered-count

<b>Syntax</b>	<b>[no] low-packets-offered-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the low packets discarded count. The <b>no</b> form of the command excludes the low packets discarded count.

## out-profile-octets-forwarded-count

<b>Syntax</b>	<b>[no] out-profile-octets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile octets forwarded count. The <b>no</b> form of the command excludes the out of profile octets forwarded count.
<b>Default</b>	no out-profile-octets-forwarded-count

## out-profile-packets-forwarded-count

<b>Syntax</b>	<b>[no] out-profile-packets-forwarded-count</b>
<b>Context</b>	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
<b>Description</b>	This command includes the out of profile packets forwarded count. The <b>no</b> form of the command excludes the out of profile packets forwarded count.
<b>Default</b>	no out-profile-packets-forwarded-count

## uncoloured-octets-offered-count

<b>Syntax</b>	<b>[no] uncoloured-packets-offered-count</b>
<b>Context</b>	config>log>acct-policy>cr>queue>i-count config>log>acct-policy>cr>ref-queue>i-count
<b>Description</b>	This command includes the uncoloured octets offered in the count. The <b>no</b> form of the command excludes the uncoloured octets offered in the count.

## uncoloured-packets-offered-count

<b>Syntax</b>	<b>[no] uncoloured-packets-offered-count</b>
<b>Context</b>	config>log>acct-policy>cr>queue>i-count config>log>acct-policy>cr>ref-queue>i-count
<b>Description</b>	This command includes the uncolored packets offered count. The <b>no</b> form of the command excludes the uncoloured packets offered count.

## ref-aa-specific-counter

<b>Syntax</b>	<b>ref-aa-specific-counter any</b> <b>no ref-aa-specific-counter</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	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 <b>no</b> 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.
<b>Parameters</b>	<b>any</b> — Indicates that a record is collected as long as any field records activity when non-zero significant-change value is configured.

## ref-override-counter

<b>Syntax</b>	<b>ref-override-counter <i>ref-override-counter-id</i></b> <b>ref-override-counter all</b> <b>no ref-override-counter</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	This command configures a reference override counter. The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no ref-override-counter

## ref-queue

<b>Syntax</b>	<b>ref-queue</b> <i>queue-id</i> <b>ref-queue all</b> <b>no ref-queue</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	This command configures a reference queue. The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no ref-queue

## significant-change

<b>Syntax</b>	<b>significant-change</b> <i>delta</i> <b>no significant-change</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	This command configures the significant change required to generate the record.
<b>Parameters</b>	<i>delta</i> — Specifies the delta change (significant change) that is required for the custom record to be written to the xml file. <b>Values</b> 0 — 4294967295 (For custom-record-aa-sub only values 0 or 1 are supported.)



## Show Commands

### accounting-policy

<b>Syntax</b>	<b>accounting-policy</b> [ <i>acct-policy-id</i> ] [ <b>access</b>   <b>network</b> ]
<b>Context</b>	show>log
<b>Description</b>	This command displays accounting policy information.
<b>Parameters</b>	<p><i>policy-id</i> — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.</p> <p><b>Values</b>      1 — 99</p> <p><b>access</b> — Only displays access accounting policies.</p> <p><b>network</b> — Only displays network accounting policies.</p>
<b>Output</b>	<b>Accounting Policy Output</b> — The following table describes accounting policy output fields.

**Table 46: Show Accounting Policy Output Fields**

Label	Description
Policy ID	The identifying value assigned to a specific policy.
Type	<p>Identifies accounting record type forwarded to the configured accounting file.</p> <p><b>access</b> — Indicates that the policy is an access accounting policy.</p> <p><b>network</b> — Indicates that the policy is a network accounting policy.</p> <p><b>none</b> — Indicates no accounting record types assigned.</p>
Def	<p><b>Yes</b> — Indicates that the policy is a default access or network policy.</p> <p><b>No</b> — Indicates that the policy is not a default access or network policy.</p>
Admin State	<p>Displays the administrative state of the policy.</p> <p><b>Up</b> — Indicates that the policy is administratively enabled.</p> <p><b>Down</b> — Indicates that the policy is administratively disabled.</p>
Oper State	<p>Displays the operational state of the policy.</p> <p><b>Up</b> — Indicates that the policy is operationally up.</p> <p><b>Down</b> — Indicates that the policy is operationally down.</p>

**Table 46: 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 Id	Type	Def	Admin State	Oper State	Intvl	File Id	Record Name
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 Id	Type	Def	Admin State	Oper State	Intvl	File Id	Record Name
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

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

10 access Yes Up Up 5 3 complete-service-ingress-egress
=====
A:ALA-1#

```

## accounting-records

<b>Syntax</b>	<b>accounting-records</b>
<b>Context</b>	show>log
<b>Description</b>	This command displays accounting policy record names.
<b>Output</b>	<b>Accounting Records Output.</b> The following table describes accounting records output fields.

**Table 47: 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

**NOTE:** aa, video and subscriber records are not applicable to the 7950 XRS.

```

A:ALA-1# show log accounting-records
=====
Accounting Policy Records
=====

```

## Show Commands

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

<b>Syntax</b>	<b>applications</b>
<b>Context</b>	show>log
<b>Description</b>	This command displays a list of all application names that can be used in event-control and filter commands.
<b>Output</b>	<b>Sample Output</b>

\*A:7950 XRS-20# show log applications

```
=====
Log Event Application Names
=====
Application Name

BGP
...
CHASSIS
...
IGMP
...
LDP
LI
...
MIRROR
...
MPLS
```

```

...
OSPF
PIM
...
PORT
...
SYSTEM
...
USER
...
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** chassis, debug, dhcp, efm\_oam, filter, gsmp, igmp\_snooping, ip, isis, lag, ldp, logger, mc\_redundancy, mirror, mpls, ntp, oam, ospf, 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.

Label	Description (Continued)
P	CL — The event has a cleared severity/priority. CR — The event has critical severity/priority. IN — The event has indeterminate severity/priority. MA — The event has major severity/priority. MI — The event has minor severity/priority. WA — The event has warning severity/priority.
g/s	gen — The event will be generated/logged by event control. sup — The event will be suppressed/dropped by event control. thr — Specifies that throttling is enabled.
Logged	The number of events logged/generated.
Dropped	The number of events dropped/suppressed.

### Sample Output

```
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

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
...
DEBUG:
L 2001 traceEvent MI gen 0 0
DOT1X:
FILTER:
 2001 filterPBRPacketsDropped MI 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 vRtrIisisDatabaseOverload WA gen 0 0
 2002 vRtrIisisManualAddressDrops WA gen 0 0
 2003 vRtrIisisCorruptedLSPDetected WA gen 0 0
 2004 vRtrIisisMaxSeqExceedAttempt WA gen 0 0
 2005 vRtrIisisIDLenMismatch WA gen 0 0
 2006 vRtrIisisMaxAreaAdrrsMismatch 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 tnnxVrrpIPListMismatch MI gen 0 0
 2004 tnnxVrrpIPListMismatchClear MI gen 0 0
 2005 tnnxVrrpMultipleOwners MI gen 0 0
 2006 tnnxVrrpBecameBackup MI gen 0 0
L 2007 vrrpPacketDiscarded MI gen 0 0
VRTR:
 2001 tnnxVRtrMidRouteTCA MI gen 0 0
 2002 tnnxVRtrHighRouteTCA MI gen 0 0
 2003 tnnxVRtrHighRouteCleared MI gen 0 0
 2004 tnnxVRtrIllegalLabelTCA MA gen 0 0
 2005 tnnxVRtrMcastMidRouteTCA MI gen 0 0
 2006 tnnxVRtrMcastMaxRoutesTCA MI gen 0 0
 2007 tnnxVRtrMcastMaxRoutesCleared MI gen 0 0
 2008 tnnxVRtrMaxArpEntriesTCA MA gen 0 0
 2009 tnnxVRtrMaxArpEntriesCleared MI gen 0 0
 2011 tnnxVRtrMaxRoutes 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

## Show Commands

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#
```

## event-handling

<b>Syntax</b>	<b>event-handling</b>
<b>Context</b>	show>log
<b>Description</b>	This command enables the context to display Event Handling System (EHS) information.

## handler

<b>Syntax</b>	<b>handler</b> [ <i>handler-name</i> ] <b>handler detail</b>
<b>Context</b>	show>log>event-handling
<b>Description</b>	This command enters the context to display EHS handler information.
<b>Parameters</b>	<i>handler-name</i> — Specifies the name of a specific handler. 32 characters maximum. <b>detail</b> — Keyword to list details of all handlers.



**Output**    **Show Handler Output** — The following table describes handler output fields.

Label	Description
Handler	The name of the handler.
Description	The handler description string.
Admin State	The administrative state of the handler.
Oper State	The operational state of the handler.

#### Handler Action-List Entry

Entry-id	The action-list entry identifier.
Description	The action-list entry description string.
Admin State	The administrative state of the action-list entry.
Policy Name	The name of the related script policy.
Policy Owner	The owner of the related script policy.
Last Exec	The timestamp of the last successful execution of the action-list entry.

#### Handler Action-List Entry Execution Statistics

Enqueued	The number of times the action-list entry was successfully passed on to the SR OS sub-system or module that will attempt to process and execute the action. For a script-policy entry, this indicates that the script request has been enqueued but does not necessarily indicate that the script has successfully launched or completed. For status and information about the script, use the <b>show&gt;system&gt;script-control</b> command.
Err Launch	The number of times the action-list entry was not successfully handed over to the next SR OS sub-system or module in the processing chain. This can be caused by a variety of conditions including a full script request input queue.
Err Adm Status	The number of times the action-list entry was not executed because the entry was administratively disabled.
Total	The total number of times that the action-list entry attempted execution.

#### Sample Output

```
A:node1>show>log>event-handling# handler
```

```
=====
Event Handling System - Handler List
=====
Handler Admin Oper Description
Name State State
=====
```

```

h-sample up up
h-main up up
h-backup down down
=====

*A:7950 XRS-20# show log event-handling handler "h-sample"

=====
Event Handling System - Handlers
=====

=====
Handler : h-sample
=====
Description : (Not Specified)
Admin State : up Oper State : up

Handler Action-List Entry

Entry-id : 10
Description : (Not Specified)
Admin State : up Oper State : up
Script
 Policy Name : sp-sample
 Policy Owner : TiMOS CLI
Min Delay : 0
Last Exec : 05/24/2015 19:03:31

Handler Action-List Entry Execution Statistics
 Enqueued : 4
 Err Launch : 0
 Err Adm Status : 0
Total : 4
=====
```

## file-id

<b>Syntax</b>	<b>file-id</b> [ <i>log-file-id</i> ]
<b>Context</b>	show>log
<b>Description</b>	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.
<b>Parameters</b>	<i>log-file-id</i> — Displays detailed information on the specified event file log.
<b>Output</b>	<b>Log File Output</b> — The following table describes the output fields for a log file summary.

Label	Description
file-id	The log file ID.
rollover	The rollover time for the log file which is how long in between partitioning of the file into a new file.
retention	The retention time for the file in the system which is how long the file should be retained in the file system.
admin location	The primary flash device specified for the file location.  none — indicates no specific flash device was specified.
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

<b>Syntax</b>	<b>filter-id</b> [ <i>filter-id</i> ]
<b>Context</b>	show>log
<b>Description</b>	This command displays event log filter policy information.
<b>Parameters</b>	<i>filter-id</i> — Displays detailed information on the specified event filter policy ID.
<b>Output</b>	<b>Event Log Filter Summary Output</b> — The following table describes the output fields for event log filter summary information.

**Table 48: 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 49: 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 50: Log Filter Match Criteria Output Fields**

Label	Description
Entry-id	The event log filter entry ID.

**Table 50: Log Filter Match Criteria Output Fields (Continued)**

Label	Description
Action	<p><code>default</code> — There is no explicit action for the event log filter entry and the filter's default action is used on matching events.</p> <p><code>drop</code> — The action for the event log filter entry is to drop matching events.</p> <p><code>forward</code> — The action for the event log filter entry is to forward matching events.</p>
Description (Entry-id)	The description string for the event log filter entry.
Application	The event log filter entry application match criterion.
Event Number	The event log filter entry application event ID match criterion.
Severity	<p><code>cleared</code> — The log event filter entry application event severity cleared match criterion.</p> <p><code>indeterminate</code> — The log event filter entry application event severity indeterminate match criterion.</p> <p><code>critical</code> — The log event filter entry application event severity critical match criterion.</p> <p><code>major</code> — The log event filter entry application event severity cleared match criterion.</p> <p><code>minor</code> — The log event filter entry application event severity minor match criterion.</p> <p><code>warning</code> — The log event filter entry application event severity warning match criterion.</p>
Subject	Displays the event log filter entry application event ID subject string match criterion.
Router	Displays the event log filter entry application event ID <b>router</b> <i>router-instance</i> string match criterion.
Operator	<p>There is an operator field for each match criteria: application, event number, severity, and subject.</p> <p><code>equal</code> — Matches when equal to the match criterion.</p>

**Table 50: Log Filter Match Criteria Output Fields (Continued)**

Label	Description
<code>greaterThan</code>	Matches when greater than the match criterion.
<code>greaterThanOrEqualTo</code>	Matches when greater than or equal to the match criterion.
<code>lessThan</code>	Matches when less than the match criterion.
<code>lessThanOrEqualTo</code>	Matches when less than or equal to the match criterion.
<code>notEqual</code>	Matches when not equal to the match criterion.
<code>off</code>	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 : greaterThanOrEqualTo
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**

<b>Syntax</b>	<b>log-collector</b>
<b>Context</b>	show>log
<b>Description</b>	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 51: Show Log-Collector Output Fields**

Label	Description
<Collector Name>	<p><b>Main</b> — The main event stream contains the events that are not explicitly directed to any other event stream.</p> <p><b>Security</b> — The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted.</p> <p><b>Change</b> — The change event stream contains all events that directly affect the configuration or operation of this node.</p> <p><b>Debug</b> — The debug-trace stream contains all messages in the debug stream.</p>
Dest. Log ID	Specifies the event log stream destination.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Status	<p><b>Enabled</b> — Logging is enabled.</p> <p><b>Disabled</b> — Logging is disabled.</p>
Dest. Type	<p><b>Console</b> — A log created with the console type destination displays events to the physical console device.</p> <p>Events are displayed to the console screen whether a user is logged in to the console or not.</p> <p><b>Session</b> — 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.</p> <p><b>Syslog</b> — Log events are sent to a syslog receiver.</p> <p><b>SNMP traps</b> — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables.</p> <p><b>File</b> — All selected log events will be directed to a file on one of the CPM's compact flash disks.</p> <p><b>Memory</b> — All selected log events will be directed to an in-memory storage area.</p>



**Sample Output**

```

A:ALA-1# show log log-collector
=====
Log Collectors
=====
Main Logged : 1224 Dropped : 0
 Dest Log Id: 99 Filter Id: 0 Status: enabled Dest Type: memory
 Dest Log Id: 100 Filter Id: 1001 Status: enabled Dest Type: memory

Security Logged : 3 Dropped : 0

Change Logged : 3896 Dropped : 0

Debug Logged : 0 Dropped : 0

=====
A:ALA-1#

```

**log-id**

<b>Syntax</b>	<b>log-id</b> [ <i>log-id</i> ] [ <b>severity</b> <i>severity-level</i> ] [ <b>application</b> <i>application</i> ] [ <b>sequence</b> <i>from-seq</i> [ <i>to-seq</i> ]] [ <b>count</b> <i>count</i> ] [ <b>router</b> <i>router-instance</i> [ <b>expression</b> ]] [ <b>message</b> <i>message</i> [ <b>regular-expression</b> ]] [ <b>subject</b> <i>subject</i> [ <b>regexp</b> ]] [ <b>ascending</b>   <b>descending</b> ] [ <b>message format</b> [ <b>msg-regexp</b> ]]
<b>Context</b>	show>log
<b>Description</b>	<p>This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.</p> <p>If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.</p> <p>If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.</p> <p>Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.</p>
<b>Parameters</b>	<p><i>log-id</i> — Displays the contents of the specified file log or memory log ID. The log ID must have a destination of an SNMP or file log or a memory log for this parameter to be used.</p> <p><b>Default</b> Displays the event log summary</p> <p><b>Values</b> 1 — 99</p> <p><b>severity</b> <i>severity-level</i> — Displays only events with the specified and higher severity.</p> <p><b>Default</b> All severity levels</p> <p><b>Values</b> cleared, indeterminate, critical, major, minor, warning</p>

**application** *application* — Displays only events generated by the specified application.

**Default** All applications

**Values** chassis, dhcp, debug, filter, ip, isis, lag, ldp, logger, mirror, mpls, oam, ospf, 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.

**message** *format* — Specifies a message string up to 400 characters to be used in the display criteria.

**msg-regexp** — Specifies to use a regular expression as parameters with the specified *message* string.

**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.

Label	Description (Continued)
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. 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 52: SNMP Trap Group Output Fields**

Label	Description
Log-ID	The log destination ID for an event stream.
Address	The IP address of the trap receiver,
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are <code>snmpv1</code> , <code>snmpv2c</code> , <code>snmpv3</code> .
Community	The community string required by <b>snmpv1</b> or <b>snmpv2c</b> trap receivers.
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 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 53: Show Log Syslog Output Fields

Label	Description
Syslog ID	The syslog ID number for the syslog destination.
IP Address	The IP address of the syslog target host.
Port	The configured UDP port number used when sending syslog messages.
Facility	The facility code for messages sent to the syslog target host.
Severity Level	The syslog message severity level threshold.
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.

**Table 53: Show Log Syslog Output Fields (Continued)**

Label	Description
Prefix Present	Yes — A log prefix was prepended to the syslog message sent to the syslog host.  No — A log prefix was not prepended to the syslog message sent to the syslog host.
Description	A text description stored in the configuration file for a configuration context.
LogPrefix	The prefix string prepended to the syslog message.
Log-id	Events are directed to this destination.

**Sample 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

<b>Syntax</b>	<b>log</b> <i>log-id</i>
<b>Context</b>	clear
<b>Description</b>	<p>Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.</p> <p>This command is only applicable to event logs that are directed to file destinations and memory destinations.</p> <p>SNMP, syslog and console/session logs are not affected by this command.</p>
<b>Parameters</b>	<i>log-id</i> . The event log ID to be initialized/rolled over.
	<b>Values</b> 1 — 100



# Standards and Protocol Support

Note that the information presented is subject to change without notice.  
Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

## Ethernet Standards

IEEE 1588 Precision Clock Synchronization Protocol  
IEEE 802.1AB Station and Media Access Control Connectivity Discovery  
IEEE 802.1ad Provider Bridges  
IEEE 802.1ag Connectivity Fault Management  
IEEE 802.1ah Provider Backbone Bridges  
IEEE 802.1ak Multiple Registration Protocol  
IEEE 802.1aq Shortest Path Bridging  
IEEE 802.1ax Link Aggregation  
IEEE 802.1D MAC Bridges  
IEEE 802.1p Traffic Class Expediting  
IEEE 802.1Q Virtual LANs  
IEEE 802.1s Multiple Spanning Trees  
IEEE 802.1w Rapid Reconfiguration of Spanning Tree  
IEEE 802.1X Port Based Network Access Control  
IEEE 802.3ab 1000BASE-T  
IEEE 802.3ac VLAN Tag  
IEEE 802.3ad Link Aggregation  
IEEE 802.3ae 10 Gb/s Ethernet  
IEEE 802.3ah Ethernet in the First Mile  
IEEE 802.3ba 40 Gb/s and 100 Gb/s Ethernet  
IEEE 802.3i Ethernet  
IEEE 802.3u Fast Ethernet  
IEEE 802.3x Ethernet Flow Control  
IEEE 802.3z Gigabit Ethernet  
ITU-T G.8031 Ethernet Linear Protection Switching  
ITU-T G.8032 Ethernet Ring Protection Switching  
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks

## OSPF

RFC 1586 Guidelines for Running OSPF Over Frame Relay Networks  
RFC 1765 OSPF Database Overflow  
RFC 2328 OSPF Version 2  
RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option  
RFC 3509 Alternative Implementations of OSPF Area Border Routers  
RFC 3623 Graceful OSPF Restart (Helper Mode)  
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2  
RFC 4203 OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)  
RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance  
RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)  
RFC 4970 Extensions to OSPF for Advertising Optional Router Capabilities  
RFC 5185 OSPF Multi-Area Adjacency  
RFC 5243 OSPF Database Exchange Summary List Optimization  
RFC 5250 The OSPF Opaque LSA Option  
RFC 5709 OSPFv2 HMAC-SHA Cryptographic Authentication  
RFC 6987 OSPF Stub Router Advertisement

## 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 2858 Multiprotocol Extensions for BGP-4  
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  
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

## Standards and Protocols

RFC 5575 Dissemination of Flow Specification Rules  
RFC 5668 4-Octet AS Specific BGP Extended Community  
draft-ietf-idr-add-paths Advertisement of Multiple Paths in BGP  
draft-ietf-idr-best-external Advertisement of the Best External Route in BGP

### IS-IS

ISO/IEC 10589:2002, Second Edition, Nov. 2002 Intermediate System to Intermediate System Intra-Domain Routing Information Exchange Protocol  
RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments  
RFC 2973 IS-IS Mesh Groups  
RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System  
RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)  
RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)  
RFC 4971 Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information  
RFC 5120 M-ISIS: Multi Topology (MT) Routing in IS-IS  
RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags  
RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS  
RFC 5302 Domain-wide Prefix Distribution with Two-Level IS-IS  
RFC 5303 Three-Way Handshake for IS-IS Point-to-Point Adjacencies  
RFC 5304 IS-IS Cryptographic Authentication  
RFC 5305 IS-IS Extensions for Traffic Engineering TE  
RFC 5306 Restart Signaling for IS-IS (Helper Mode)  
RFC 5307 IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)

RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols  
RFC 5310 IS-IS Generic Cryptographic Authentication  
RFC 6213 IS-IS BFD-Enabled TLV  
RFC 6329 IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging  
draft-ietf-isis-mi-02 IS-IS Multi-Instance

### IP, LDP, and Segment Routing Fast Reroute (FRR)

RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates  
draft-ietf-isis-segment-routing-extensions-03 IS-IS Extensions for Segment Routing  
draft-ietf-rtgwg-lfa-manageability-07 Operational management of Loop Free Alternates  
draft-ietf-rtgwg-remote-lfa-09 Remote LFA FRR  
draft-kratn-mofrr-02 Multicast only Fast Re-Route

### IPSec

RFC 2401 Security Architecture for the Internet Protocol  
RFC 2406 IP Encapsulating Security Payload (ESP)  
RFC 2409 The Internet Key Exchange (IKE)  
RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP  
RFC 3706 IKE Dead Peer Detection  
RFC 3947 Negotiation of NAT-Traversal in the IKE  
RFC 3948 UDP Encapsulation of IPsec ESP Packets  
RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)  
RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)  
RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)  
RFC 5998 An Extension for EAP-Only Authentication in IKEv2

draft-ietf-ipsec-isakmp-xauth-06 Extended Authentication within ISAKMP/Oakley (XAUTH)  
draft-ietf-ipsec-isakmp-modecfg-05 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 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 IPv6  
RFC 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  
RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol  
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6  
RFC 3971 SEcure Neighbor Discovery (SEND)  
RFC 3972 Cryptographically Generated Addresses (CGA)  
RFC 4007 IPv6 Scoped Address Architecture  
RFC 4193 Unique Local IPv6 Unicast Addresses  
RFC 4291 IPv6 Addressing Architecture  
RFC 4443 Internet Control Message Protocol (ICMPv6)  
for the Internet Protocol Version 6 (IPv6) Specification  
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  
 RFC 5187 OSPFv3 Graceful Restart (Helper Mode)  
 RFC 5308 Routing IPv6 with IS-IS  
 RFC 5340 OSPF for IPv6  
 RFC 5838 Support of Address Families in OSPFv3

### **Multicast**

RFC 1112 Host Extensions for IP Multicasting (Snooping)  
 RFC 2236 Internet Group Management Protocol, (Snooping)  
 RFC 2362 Protocol Independent Multicast-Sparse Mode (PIMSM)  
 RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)  
 RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)  
 RFC 3618 Multicast Source Discovery Protocol (MSDP)  
 RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address  
 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 4624 Multicast Source Discovery Protocol (MSDP) MIB  
 RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)  
 RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

RFC 5384 The Protocol Independent Multicast (PIM) Join Attribute Format  
 RFC 5496 The Reverse Path Forwarding (RPF) Vector TLV  
 RFC 6037 Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs  
 RFC 6513 Multicast in MPLS/BGP IP VPNs  
 RFC 6514 BGP Encodings and Procedures for Multicast in MPLS/IP VPNs  
 RFC 6515 IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs  
 RFC 6516 IPv6 Multicast MVPN Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages  
 RFC 6625 Wildcards in Multicast VPN Auto-Discover Routes  
 RFC 6826 Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path  
 RFC 7246 Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF)  
 RFC 7385 IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points  
 draft-dolganow-l3vpn-mvpn-expl-track-00 Explicit tracking in MPLS/BGP IP VPN

### **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 3140 Per-Hop Behavior Identification Codes  
 RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks

RFC 4023 Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)  
 RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL  
 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  
 RFC 5561 LDP Capabilities  
 RFC 6388 LDP Extensions for Point-to-Multipoint and Multipoint-to-Multipoint LSP  
 RFC 6826 Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths  
 draft-ietf-mpls-ldp-ip-pw-capability-09 Disabling IPoMPLS and P2P PW LDP Application's State Advertisement  
 draft-ietf-mpls-ldp-ipv6-15 Updates to LDP for IPv6  
 draft-pdutta-mpls-ldp-adj-capability-00 LDP Adjacency Capabilities  
 draft-pdutta-mpls-ldp-v2-00 LDP Version 2  
 draft-pdutta-mpls-multi-ldp-instance-00 Multiple LDP Instances  
 draft-pdutta-mpls-tldp-hello-reduce-04 Targeted LDP Hello Reduction

### **MPLS/RSVP — TE**

RFC 2702 Requirements for Traffic Engineering over MPLS  
 RFC2747 RSVP Cryptographic Authentication  
 RFC 2961 RSVP Refresh Overhead Reduction Extensions  
 RFC3097 RSVP Cryptographic Authentication - Updated Message Type Value  
 RFC 3209 Extensions to RSVP for Tunnels

RFC 3473 Generalized Multi-Protocol Label Switching (GMPLS) Signaling

Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions – (support of of IF\_ID RSVP\_HOP object with unnumbered interface and RSVP-TE Graceful Restart Helper Procedures)

RFC 3477 Signalling Unnumbered Links in Resource Reservation Protocol-Traffic Engineering (RSVP-TE)

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 4950 ICMP Extensions for Multiprotocol Label Switching

RFC 5151 Inter-domain MPLS and GMPLS Traffic Engineering – RSVP-TE Extensions

RFC 5712 MPLS Traffic Engineering Soft Preemption

RFC 5817 Graceful Shutdown in GMPLS Traffic Engineering Networks

draft-newton-mpls-te-dynamic-overbooking-00 A Diffserv-TE Implementation Model to dynamically change booking factors during failure events

### MPLS — OAM

RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

RFC 6424 Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

RFC 6425 Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping

### MPLS — TP (7750/7450 only)

RFC 5586 MPLS Generic Associated Channel

RFC 5921 A Framework for MPLS in Transport Networks

RFC 5960 MPLS Transport Profile Data Plane Architecture

RFC 6370 MPLS-TP Identifiers

RFC 6378 MPLS-TP Linear Protection

RFC 6428 Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile

RFC 6426 MPLS On-Demand Connectivity and Route Tracing

RFC 6478 Pseudowire Status for Static Pseudowires

RFC 7213 MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing

### MPLS — GMPLS

RFC 3471 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description

RFC 3473 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions

RFC 4204 Link Management Protocol (LMP)

RFC 4208 Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model

RFC 4872 RSVP-TE Extensions in Support of End to End GMPLS recovery

draft-ietf-ccamp-rsvp-te-srlg-collect-04 RSVP-TE Extensions for Collecting SRLG Information

### RIP

RFC 1058 RIP Version 1

RFC 2080 RIPng for IPv6

RFC 2082 RIP-2 MD5 Authentication

RFC 2453 RIP Version 2

### TCP/IP

RFC 768 UDP

RFC 791 IP

RFC 792 ICMP

RFC 793 TCP

RFC 826 ARP

RFC 854 Telnet

RFC 951 Bootstrap Protocol (BOOTP)

RFC 1350 The Tftp Protocol (revision 2)

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

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

draft-ietf-vrrp-unified-spec-02 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

**PPP**

RFC 1332 PPP IPCP  
 RFC 1377 PPP OSINLCP  
 RFC 1638/2878 PPP 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 2516 A Method for Transmitting PPP Over Ethernet  
 RFC 2615 PPP over SONET/SDH  
 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

**Policy Management and Credit Control**

3GPP TS 29.212 Policy and Charging Control (PCC) over Gx/Sd Reference Point (Release 11 and Release 12) - Gx support as it applies to wireline environment (BNG)  
 RFC 3588 Diameter Base Protocol  
 RFC 4006 Diameter Credit Control Application

**NAT**

RFC 5382 NAT Behavioral Requirements for TCP  
 RFC 5508 NAT Behavioral Requirements for ICMP

RFC 6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers  
 RFC 6333 Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion  
 RFC 6334 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite  
 RFC 6888 Common Requirements For Carrier-Grade NATs (CGNs)

**VPLS**

RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling  
 RFC 4762 Virtual Private LAN Services Using LDP  
 RFC 5501 Requirements for Multicast Support in Virtual Private LAN Services  
 RFC 6074 Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)  
 RFC 7041 Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging  
 RFC 7117 Multicast in Virtual Private LAN Service (VPLS)

**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  
 RFC 4816 PWE3 ATM Transparent Cell Transport Service  
 RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks  
 RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks  
 RFC 4446 IANA Allocations for PWE3  
 RFC 4447 Pseudowire Setup and Maintenance Using LDP

## Standards and Protocols

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  
RFC 5885 Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)  
RFC 6073 Segmented Pseudowire  
RFC 6310 Pseudowire (PW) OAM Message Mapping  
RFC 6391 Flow Aware Transport of Pseudowires over an MPLS PSN  
RFC 6575 ARP Mediation for IP Interworking of Layer 2 VPN  
RFC 6718 Pseudowire Redundancy  
RFC 6829 Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6  
RFC 6870 Pseudowire Preferential Forwarding Status bit  
RFC 7023 MPLS and Ethernet OAM Interworking  
RFC 7267 Dynamic Placement of Multi-Segment Pseudowires  
draft-ietf-l2vpn-vpws-iw-oam-04 OAM Procedures for VPWS Interworking  
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

RFC 5851 ANCP framework  
draft-ietf-ancp-protocol-02 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-T G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1 issued in July 2002

### AAA

RFC 2865 Remote Authentication Dial In User Service  
RFC 2866 RADIUS Accounting  
draft-grant-tacacs-02 The TACACS+ Protocol

### SSH

RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers  
RFC 4251 The Secure Shell (SSH) Protocol Architecture

RFC 4254 The Secure Shell (SSH) Connection Protocol

### OpenFlow

ONF OpenFlow Switch Specification Version 1.3.1 (Hybrid-switch/FlowTable)

### 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.  
ITU-T G.8265.1 Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010.  
IEEE 1588-2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

**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 2138 RADIUS

RFC 2206 RSVP-MIB

RFC 2452 IPv6 Management Information  
Base for the Transmission Control  
Protocol

RFC 2465 Management Information  
Base for IPv6: Textual Conventions  
and General Group

RFC 2558 SONET-MIB

RFC 2571 SNMP-FRAMEWORKMIB

RFC 2572 SNMP-MPD-MIB

RFC 2573 SNMP-TARGET-&-  
NOTIFICATION-MIB

RFC 2574 SNMP-USER-BASED-  
SMMIB

RFC 2575 SNMP-VIEW-BASED-ACM-  
MIB

RFC 2576 SNMP-COMMUNITY-MIB

RFC 2578 Structure of Management  
Information Version 2 (SMIv2)

RFC 2665 EtherLike-MIB

RFC 2819 RMON-MIB

RFC 2863 IF-MIB

RFC 2864 INVERTED-STACK-MIB

RFC 2987 VRRP-MIB

RFC 3014 NOTIFICATION-LOGMIB

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 3826 The Advanced Encryption  
Standard (AES) Cipher Algorithm in  
the SNMP User-based Security  
Model

RFC 4113 Management Information  
Base for the User Datagram Protocol  
(UDP)

RFC 4292 IP Forwarding Table 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

RFC 6241 Network Configuration  
Protocol (NETCONF)

RFC 6242 Using the NETCONF Protocol  
over Secure Shell (SSH)

draft-ietf-bfd-mib-00 Bidirectional  
Forwarding Detection Management  
Information Base

draft-ietf-isis-wg-mib-06 Management  
Information Base for Intermediate  
System to Intermediate System (IS-  
IS)

draft-ietf-ospf-mib-update-04 OSPF  
Version 2 Management Information  
Base

draft-ietf-mboned-msdp-mib-01  
Multicast Source Discovery protocol  
MIB

draft-ietf-mppls-lsr-mib-06 Multiprotocol  
Label Switching (MPLS) Label  
Switching Router (LSR)  
Management Information Base

draft-ietf-mppls-te-mib-04 Multiprotocol  
Label Switching (MPLS) Traffic  
Engineering Management  
Information Base

draft-ietf-mppls-ldp-mib-07 Definitions of  
Managed Objects for the  
Multiprotocol Label Switching,  
Label Distribution Protocol (LDP)

IEEE 802.3ad MIB





# Customer documentation and product support



## Customer documentation

<http://documentation.alcatel-lucent.com>



## Technical support

<http://support.alcatel-lucent.com>



## Documentation feedback

[documentation.feedback@alcatel-lucent.com](mailto:documentation.feedback@alcatel-lucent.com)

