



**7450 ETHERNET SERVICE SWITCH  
7750 SERVICE ROUTER  
7950 EXTENSIBLE ROUTING SYSTEM  
VIRTUALIZED SERVICE ROUTER**

**SYSTEM MANAGEMENT GUIDE  
RELEASE 16.0.R5**

**3HE 14139 AAAC TQZZA 01**

**Issue: 01**

**December 2018**

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2018 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

# Table of Contents

<b>1</b>	<b>Getting Started .....</b>	<b>13</b>
1.1	About This Guide .....	13
1.2	Router Configuration Process .....	15
<b>2</b>	<b>Security .....</b>	<b>17</b>
2.1	Authentication, Authorization, and Accounting .....	17
2.1.1	Authentication .....	18
2.1.1.1	Local Authentication .....	19
2.1.1.2	RADIUS Authentication .....	20
2.1.1.3	TACACS+ Authentication .....	24
2.1.1.4	LDAP Authentication .....	25
2.1.2	Authorization .....	32
2.1.2.1	Local Authorization .....	32
2.1.2.2	RADIUS Authorization .....	32
2.1.2.3	TACACS+ Authorization .....	33
2.1.2.4	Authorization Profiles for Different Interfaces .....	35
2.1.2.5	Authorization Support .....	36
2.1.3	Accounting .....	37
2.1.3.1	RADIUS Accounting .....	37
2.1.3.2	TACACS+ Accounting .....	37
2.2	Security Controls .....	39
2.2.1	When a Server Does Not Respond .....	39
2.2.2	Access Request Flow .....	40
2.3	Control and Management Traffic Protection .....	41
2.3.1	CPM Filters .....	41
2.3.1.1	CPM Filter Packet Match .....	41
2.3.1.2	CPM IPv4 and IPv6 Filter Entry Match Criteria .....	42
2.3.1.3	CPM MAC Filter Entry Match Criteria .....	44
2.3.1.4	CPM Filter Policy Action .....	45
2.3.1.5	CPM Filter Policy Statistics and Logging .....	45
2.3.1.6	CPM Filter: Protocols and Ports .....	45
2.3.2	CPM Per-Peer Queuing .....	50
2.3.3	Centralized CPU Protection .....	50
2.3.3.1	Protocol Protection .....	52
2.3.3.2	CPU Protection Extensions for ETH-CFM .....	53
2.3.3.3	ETH-CFM Ingress Squelching .....	55
2.3.4	Distributed CPU Protection (DCP) .....	58
2.3.4.1	Applicability of Distributed CPU Protection .....	60
2.3.4.2	Log Events, Statistics, Status, and SNMP support .....	61
2.3.4.3	DCP Policer Resource Management .....	61
2.3.4.4	Operational Guidelines and Tips .....	62
2.3.5	Classification-Based Priority for Extracted Protocol Traffic .....	64
2.3.6	TTL Security .....	65
2.3.7	Management Access Filter .....	66
2.3.7.1	MAF Filter Packet Match .....	66

2.3.7.2	MAF IPv4/IPv6 Filter Entry Match Criteria .....	67
2.3.7.3	MAF MAC Filter Entry Match Criteria .....	67
2.3.7.4	MAF Filter Policy Action .....	68
2.3.7.5	MAF Filter Policy Statistics and Logging .....	68
2.4	Vendor-Specific Attributes (VSAs).....	69
2.5	Other Security Features .....	70
2.5.1	Secure Shell (SSH) .....	70
2.5.2	SSH PKI Authentication.....	71
2.5.2.1	Key Generation.....	72
2.5.3	HMAC strengthening (SHA-224/256/384/512) .....	72
2.5.4	MAC Client and Server List .....	73
2.5.5	Regenerate the ssh-key without disabling SSH .....	73
2.5.5.1	Key re-exchange procedure .....	74
2.5.6	Exponential Login Backoff .....	75
2.5.7	User Lockout .....	76
2.5.8	CLI Login Scripts .....	76
2.5.9	802.1x Network Access Control .....	77
2.5.10	TCP Enhanced Authentication Option.....	77
2.5.10.1	Packet Formats .....	77
2.5.10.2	Keychain.....	79
2.5.11	gRPC Authentication .....	81
2.5.12	Hash Management per Management Interface Configuration.....	83
2.5.12.1	Hash encryption Using AES 256 .....	83
2.5.12.2	Clear Text.....	84
2.6	Configuration Notes.....	85
2.6.1	General.....	85
2.7	Configuring Security with CLI .....	87
2.7.1	Security Configurations .....	87
2.7.2	Security Configuration Procedures.....	88
2.7.2.1	Configuring Management Access Filters.....	88
2.7.2.2	Configuring IP CPM Filters .....	89
2.7.2.3	Configuring IPv6 CPM Filters .....	90
2.7.2.4	Configuring MAC CPM Filters .....	92
2.7.2.5	Configuring CPM Queues.....	92
2.7.2.6	IPSec Certificates Parameters .....	93
2.7.2.7	Configuring Profiles .....	94
2.7.2.8	Configuring Users.....	100
2.7.2.9	Configuring Keychains.....	100
2.7.2.10	Copying and Overwriting Users and Profiles.....	101
2.7.3	RADIUS Configurations.....	104
2.7.3.1	Configuring RADIUS Authentication.....	104
2.7.3.2	Configuring RADIUS Authorization.....	105
2.7.3.3	Configuring RADIUS Accounting.....	106
2.7.4	Configuring 802.1x RADIUS Policies .....	107
2.7.5	TACACS+ Configurations.....	107
2.7.5.1	Enabling TACACS+ Authentication .....	107
2.7.5.2	Configuring TACACS+ Authorization .....	108
2.7.5.3	Configuring TACACS+ Accounting.....	109
2.7.5.4	Enabling SSH .....	109

2.7.6	LDAP Configurations .....	110
2.7.6.1	Configuring LDAP Authentication .....	110
2.7.6.2	Configuring Redundant Servers .....	111
2.7.6.3	Enabling SSH .....	112
2.7.7	Configuring Login Controls .....	112
2.8	Security Configuration Command Reference .....	113
2.8.1	Command Hierarchies .....	113
2.8.1.1	Security Commands .....	113
2.8.1.2	Login Control Commands .....	131
2.8.2	Command Descriptions .....	132
2.8.2.1	General Security Commands .....	133
2.8.2.2	Security Commands .....	134
2.8.2.3	LLDP Commands .....	148
2.8.2.4	Management Access Filter Commands .....	151
2.8.2.5	CLI Script Authorization Commands .....	166
2.8.2.6	CPM Filter Commands .....	167
2.8.2.7	CPM Queue Commands .....	185
2.8.2.8	CPU Protection Commands .....	187
2.8.2.9	Distributed CPU Protection Commands .....	196
2.8.2.10	Extracted Protocol Traffic Priority Commands .....	204
2.8.2.11	Security Password Commands .....	205
2.8.2.12	Public Key Infrastructure (PKI) Commands .....	216
2.8.2.13	Profile Commands .....	233
2.8.2.14	CLI Session Commands .....	238
2.8.2.15	RADIUS Commands .....	240
2.8.2.16	TACACS+ Client Commands .....	244
2.8.2.17	LDAP Client Commands .....	249
2.8.2.18	User Management Commands .....	253
2.8.2.19	Dot1x Commands .....	263
2.8.2.20	Keychain Authentication .....	266
2.8.2.21	TTL Security Commands .....	272
2.8.2.22	gRPC Commands .....	273
2.8.2.23	Login Control Commands .....	278
2.9	Security Show, Clear, Debug, Tools, and Admin Command Reference .....	285
2.9.1	Command Hierarchies .....	285
2.9.1.1	Show Commands .....	285
2.9.1.2	Clear Commands .....	286
2.9.1.3	Debug Commands .....	287
2.9.1.4	Tools Commands .....	287
2.9.1.5	Admin Commands .....	288
2.9.2	Command Descriptions .....	288
2.9.2.1	Show Commands .....	289
2.9.2.2	Clear Commands .....	345
2.9.2.3	Debug Commands .....	347
2.9.2.4	Tools Commands .....	349
2.9.2.5	Admin Commands .....	351

<b>3</b>	<b>Classic and Model-Driven Management Interfaces .....</b>	<b>353</b>
3.1	Model-Driven Management Interfaces .....	353
3.1.1	Prerequisites for Using Model-Driven Management Interfaces .....	355
3.2	YANG Data Models .....	356
3.2.1	SR OS YANG Data Models .....	356
3.2.2	OpenConfig YANG Data Models .....	358
3.3	System-Provisioned Configuration (SPC) Objects .....	362
3.4	Management Interface Configuration Mode .....	364
3.4.1	Mixed Configuration Mode .....	365
3.4.2	Loose References to IDs .....	366
3.4.3	Transitioning Between Modes .....	369
3.5	Configuring the CLI Engine .....	370
3.6	Classic and Model-Driven Management Interfaces Command Reference .....	373
3.6.1	Command Hierarchies .....	373
3.6.1.1	Management Infrastructure Control Commands .....	373
3.6.2	Command Descriptions .....	374
3.6.2.1	Management Infrastructure Control Commands .....	374
3.7	Classic and Model-Driven Management Interfaces Show Command Reference .....	383
3.7.1	Command Hierarchies .....	383
3.7.1.1	Management Infrastructure Show Commands .....	383
3.7.2	Command Descriptions .....	383
3.7.2.1	Management Infrastructure Show Commands .....	383
<b>4</b>	<b>SNMP .....</b>	<b>387</b>
4.1	SNMP Overview .....	387
4.1.1	SNMP Architecture .....	387
4.1.2	Management Information Base .....	388
4.1.3	SNMP Protocol Operations .....	388
4.1.4	SNMP Versions .....	388
4.1.5	Management Information Access Control .....	389
4.1.6	User-Based Security Model Community Strings .....	389
4.1.7	Views .....	390
4.1.8	Access Groups .....	390
4.1.9	Users .....	391
4.1.10	Per-VRN Logs and SNMP Access .....	391
4.1.11	Per-SNMP Community Source IP Address Validation .....	392
4.2	SNMP Versions .....	393
4.3	Configuration Notes .....	395
4.3.1	General .....	395
4.4	Configuring SNMP with CLI .....	397
4.4.1	SNMP Configuration Overview .....	397
4.4.1.1	Configuring SNMPv1 and SNMPv2c .....	397
4.4.1.2	Configuring SNMPv3 .....	397
4.4.2	Basic SNMP Security Configuration .....	398
4.4.3	Configuring SNMP Components .....	399
4.4.3.1	Configuring a Community String .....	399
4.4.3.2	Configuring View Options .....	400

4.4.3.3	Configuring Access Options .....	400
4.4.3.4	Configuring USM Community Options.....	401
4.4.3.5	Configuring Other SNMP Parameters .....	402
4.5	SNMP Configuration Command Reference.....	403
4.5.1	Command Hierarchies .....	403
4.5.1.1	SNMP System Commands.....	403
4.5.1.2	SNMP Security Commands.....	403
4.5.2	Command Descriptions .....	404
4.5.2.1	SNMP System Commands.....	404
4.5.2.2	SNMP Security Commands.....	407
4.6	SNMP Show Command Reference .....	415
4.6.1	Command Hierarchies .....	415
4.6.1.1	Show Commands .....	415
4.6.2	Command Descriptions .....	415
4.6.2.1	Show Commands .....	415
<b>5</b>	<b>NETCONF .....</b>	<b>437</b>
5.1	NETCONF Overview .....	437
5.2	NETCONF in SR OS .....	439
5.2.1	Transport and Sessions.....	439
5.2.2	Datastores and URLs .....	441
5.2.3	NETCONF Operations and Capabilities .....	442
5.2.3.1	<get> .....	445
5.2.3.2	<get-config>.....	446
5.2.3.3	<edit-config> .....	446
5.2.3.4	<copy-config> and <delete-config> .....	447
5.2.3.5	<lock> .....	448
5.2.3.6	<unlock> .....	449
5.2.3.7	<commit> .....	449
5.2.3.8	<discard-changes> .....	452
5.2.3.9	<validate> .....	452
5.2.3.10	<get-schema> .....	452
5.2.4	Data Model, Datastore and Operation Combinations.....	452
5.2.5	General NETCONF Behavior .....	453
5.3	Establishing a NETCONF Session .....	464
5.4	XML Content Layer.....	466
5.4.1	<get> with XML Content Layer .....	466
5.4.2	<edit-config> with XML Content Layer .....	468
5.4.3	<get-config> with XML Content Layer .....	477
5.4.4	XML Content Layer Examples .....	482
5.5	CLI Content Layer .....	486
5.5.1	CLI Content Layer Examples .....	487
5.6	NETCONF Notifications.....	492
5.7	NETCONF Monitoring .....	499
5.8	YANG Library .....	503
5.9	NETCONF Configuration Command Reference.....	505
5.9.1	Command Hierarchies.....	505
5.9.1.1	NETCONF System Commands.....	505
5.9.1.2	NETCONF Security Commands.....	505

5.9.2	Configuration Commands .....	505
5.9.2.1	NETCONF System Commands .....	506
5.9.2.2	NETCONF Security Commands .....	507
5.10	NETCONF Show and Debug Command Reference .....	509
5.10.1	Command Hierarchies .....	509
5.10.1.1	Show Commands .....	509
5.10.1.2	Debug Commands .....	509
5.10.2	Command Descriptions .....	509
5.10.2.1	Show Commands .....	509
5.10.3	Debug Commands .....	512
5.10.3.1	NETCONF Debug Commands .....	512
5.11	NETCONF Admin Command Reference .....	515
5.11.1	Command Hierarchies .....	515
5.11.1.1	Admin Commands .....	515
5.11.2	Command Descriptions .....	515
5.11.2.1	Admin Commands .....	515
<b>6</b>	<b>Event and Accounting Logs .....</b>	<b>517</b>
6.1	Logging Overview .....	517
6.2	Log Destinations .....	519
6.2.1	Console .....	519
6.2.2	Session .....	519
6.2.3	CLI Logs .....	520
6.2.4	Memory Logs .....	520
6.2.5	Log Files .....	520
6.2.6	SNMP Trap Group .....	522
6.2.7	Syslog .....	523
6.2.8	NETCONF .....	525
6.3	Event Logs .....	526
6.3.1	Event Sources .....	526
6.3.2	Event Control .....	528
6.3.3	Log Manager and Event Logs .....	529
6.3.4	Event Filter Policies .....	529
6.3.5	Event Log Entries .....	530
6.3.6	Simple Logger Event Throttling .....	532
6.3.7	Default System Log .....	533
6.3.8	Event Handling System .....	533
6.3.8.1	Executing EHS/CRON Scripts .....	541
6.4	Customizing Syslog Messages Using Python .....	543
6.4.1	Python Engine for Syslog .....	543
6.4.1.1	Python Syslog APIs .....	544
6.4.1.2	Timestamp Format Manipulation .....	547
6.4.2	Python Processing Efficiency .....	548
6.4.3	Python Backpressure .....	549
6.4.4	Event Selection for Python Processing .....	549
6.4.5	Modifying a Log File .....	550
6.4.6	Deleting a Log File .....	551
6.4.7	Modifying a File ID .....	552
6.4.8	Modifying a Syslog ID .....	553



6.4.9	Modifying an SNMP Trap Group .....	554
6.4.10	Deleting an SNMP Trap Group.....	554
6.4.11	Modifying a Log Filter .....	555
6.4.12	Modifying Event Control Parameters.....	556
6.4.13	Returning to the Default Event Control Configuration .....	557
6.5	Accounting Logs .....	559
6.5.1	Accounting Records .....	559
6.5.2	Accounting Files .....	582
6.5.3	Design Considerations .....	582
6.5.4	Reporting and Time-Based Accounting.....	583
6.5.5	Overhead Reduction in Accounting: Custom Record .....	583
6.5.5.1	User Configurable Records .....	583
6.5.5.2	Changed Statistics Only .....	584
6.5.5.3	Configurable Accounting Records .....	584
6.5.5.4	Significant Change Only Reporting .....	584
6.5.6	Immediate Completion of Records .....	585
6.5.6.1	Record Completion for XML Accounting .....	585
6.5.7	AA Accounting per Forwarding Class.....	585
6.6	Configuration Notes.....	586
6.7	Configuring Logging with CLI .....	587
6.7.1	Log Configuration Overview .....	587
6.7.2	Log Types.....	587
6.7.3	Basic Log Configuration .....	588
6.7.4	Common Configuration Tasks .....	588
6.7.4.1	Configuring an Event Log .....	588
6.7.4.2	Configuring a File ID.....	589
6.7.4.3	Configuring an Accounting Policy.....	590
6.7.4.4	Configuring Event Control .....	591
6.7.4.5	Configuring a Log Filter .....	591
6.7.4.6	Configuring an SNMP Trap Group .....	592
6.7.4.7	Configuring a Syslog Target.....	597
6.8	Log Configuration Command Reference .....	601
6.8.1	Command Hierarchies.....	601
6.8.1.1	Log Configuration Commands .....	601
6.8.1.2	Accounting Policy Commands.....	602
6.8.1.3	Custom Record Commands .....	602
6.8.1.4	File ID Commands.....	605
6.8.1.5	Event Filter Commands .....	605
6.8.1.6	Event Handling System (EHS) Commands .....	606
6.8.1.7	Event Trigger Commands.....	606
6.8.1.8	Log ID Commands.....	607
6.8.1.9	SNMP Trap Group Commands .....	607
6.8.1.10	Syslog Commands .....	608
6.8.2	Command Descriptions .....	608
6.8.2.1	Generic Commands.....	609
6.8.2.2	Log Configuration Commands .....	610
6.8.2.3	Accounting Policy Commands.....	615
6.8.2.4	File ID Commands.....	639
6.8.2.5	Event Filter Commands .....	642

6.8.2.6	Event Handling System (EHS) Commands .....	649
6.8.2.7	Event Trigger Commands.....	651
6.8.2.8	Log ID Commands.....	653
6.8.2.9	SNMP Trap Groups .....	660
6.8.2.10	Syslog Commands .....	664
6.9	Log Command Reference .....	671
6.9.1	Command Hierarchies.....	671
6.9.1.1	Show Commands .....	671
6.9.1.2	Clear Command .....	671
6.9.1.3	Tools Commands .....	672
6.9.2	Command Descriptions .....	672
6.9.2.1	Show Commands .....	672
6.9.2.2	Clear Commands.....	702
6.9.2.3	Tools Commands .....	703
<b>7</b>	<b>sFlow .....</b>	<b>707</b>
7.1	sFlow Overview .....	707
7.2	sFlow Features .....	708
7.2.1	sFlow Counter Polling Architecture .....	708
7.2.2	sFlow Support on Logical Ethernet Ports .....	709
7.2.3	sFlow SAP Counter Map .....	710
7.2.4	sFlow Record Formats .....	710
7.3	sFlow Command Reference .....	715
7.3.1	Command Hierarchies.....	715
7.3.1.1	System Commands .....	715
7.3.1.2	Show Commands .....	715
7.4	sFlow Configuration Command Descriptions .....	717
7.4.1	Command Descriptions .....	717
7.4.1.1	System Commands .....	717
7.5	sFlow Show Command Descriptions.....	721
7.5.1	Command Descriptions .....	721
7.5.1.1	Show Commands .....	721
<b>8</b>	<b>gRPC .....</b>	<b>725</b>
8.1	Security Aspects.....	726
8.1.1	TLS-Based Encryption.....	726
8.1.2	Authentication.....	726
8.2	gNMI Service .....	728
8.2.1	gNMI Service Definitions .....	728
8.2.1.1	Capability Discovery .....	728
8.2.1.2	Get/Set RPC.....	729
8.2.1.3	Subscribe RPC .....	730
8.2.1.4	Schema Paths .....	732
8.2.2	gNMI Service Use Cases .....	734
8.2.2.1	Telemetry.....	734
8.2.2.2	NE Configuration Management .....	740
8.3	gRPC Command Reference.....	743
8.3.1	Command Hierarchies.....	743
8.3.1.1	System Commands .....	743

8.3.1.2	QoS Commands .....	743
8.4	Telemetry Configuration Command Descriptions .....	745
8.4.1	Command Descriptions .....	745
8.4.1.1	System Commands .....	745
8.4.1.2	QoS Commands .....	746
8.5	gRPC Show, Admin Command Reference .....	747
8.5.1	Command Hierarchies .....	747
8.5.1.1	Show Commands .....	747
8.5.1.2	Tools Commands .....	747
8.5.1.3	Admin Commands .....	748
8.5.2	Command Descriptions .....	748
8.5.2.1	Show Commands .....	748
8.5.2.2	Tools Commands .....	750
8.5.2.3	Admin Commands .....	755
<b>9</b>	<b>TLS .....</b>	<b>757</b>
9.1	TLS Overview .....	757
9.2	TLS Server Interaction with Applications .....	758
9.2.1	TLS Application Support .....	758
9.3	TLS Handshake .....	759
9.4	TLS Client Certificate .....	761
9.5	TLS Symmetric Key Rollover .....	762
9.6	Supported TLS Ciphers .....	763
9.7	SR OS Certificate Management .....	764
9.7.1	Certificate Profile .....	764
9.7.2	TLS Server Authentication of the Client Certificate CN Field .....	765
9.7.3	CN Regexp Format .....	765
9.8	Operational Guidelines .....	766
9.8.1	Server Authentication Behavior .....	766
9.8.2	Client TLS Profile and Trust Anchor Behavior and Scale .....	767
9.9	LDAP Redundancy and TLS .....	768
9.10	Basic TLS Configuration .....	771
9.11	Common Configuration Tasks .....	773
9.11.1	Configuring a Server TLS Profile .....	773
9.11.2	Configuring a Client TLS Profile .....	773
9.11.3	Configuring a TLS Client or TLS Server Certificate .....	773
9.11.4	Configuring a TLS Trust Anchor .....	774
9.12	TLS Command Reference .....	777
9.12.1	Command Hierarchies .....	777
9.12.1.1	Security TLS Commands .....	777
9.12.1.2	LDAP TLS Profile Commands .....	778
9.12.1.3	Admin Commands .....	778
9.12.2	Command Descriptions .....	778
9.12.2.1	Security TLS Commands .....	779
9.12.2.2	LDAP TLS Profile Commands .....	786
9.12.2.3	Admin Commands .....	787
9.13	TLS Show Command Reference .....	789
9.13.1	Command Hierarchies .....	789
9.13.1.1	Show Commands .....	789

---

9.13.2	Command Descriptions .....	789
9.13.2.1	Show Commands .....	789
<b>10</b>	<b>Facility Alarms .....</b>	<b>793</b>
10.1	Facility Alarms Overview .....	793
10.2	Facility Alarms vs. Log Events .....	794
10.3	Facility Alarm Severities and Alarm LED Behavior.....	796
10.4	Facility Alarm Hierarchy.....	797
10.5	Facility Alarm List .....	798
10.6	Configuring Logging with CLI .....	811
10.6.1	Basic Facility Alarm Configuration.....	811
10.6.2	Common Configuration Tasks .....	811
10.6.2.1	Configuring the Maximum Number of Alarms to Clear .....	811
10.7	Facility Alarms Configuration Command Reference.....	813
10.7.1	Command Hierarchies.....	813
10.7.1.1	Facility Alarm Configuration Commands .....	813
10.7.2	Command Descriptions .....	813
10.7.2.1	Generic Commands.....	813
10.8	Facility Alarms Show Command Reference .....	815
10.8.1	Command Hierarchies.....	815
10.8.1.1	Show Commands .....	815
10.8.2	Command Descriptions .....	815
10.8.2.1	Show Commands .....	815
<b>11</b>	<b>Standards and Protocol Support .....</b>	<b>817</b>

# 1 Getting Started

## 1.1 About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure SR-OS boot option file (BOF), file system and system management functions.

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.

The topics and commands described in this document apply to the:

- 7450 ESS
- 7750 SR
- 7950 XRS
- VSR

[Table 1](#) lists the available chassis types for each SR OS router.

**Table 1 Supported SR OS Router Chassis Types**

7450 ESS	7750 SR	7950 XRS
<ul style="list-style-type: none"> <li>• 7450 ESS-7/12 running in standard mode (not mixed-mode)</li> </ul>	<ul style="list-style-type: none"> <li>• 7450 ESS-7/12 running in mixed-mode (not standard mode)</li> <li>• 7750 SR-a4/a8</li> <li>• 7750 SR-c4/c12</li> <li>• 7750 SR-1e/2e/3e</li> <li>• 7750 SR-7/12</li> <li>• 7750 SR-12e</li> <li>• 7750 SR-7s/14s</li> <li>• 7750 SR-1</li> </ul>	<ul style="list-style-type: none"> <li>• 7950 XRS-16c</li> <li>• 7950 XRS-20/40</li> </ul>

For a list of unsupported features by platform and chassis, refer to the *SR OS 16.0.Rx Software Release Notes*, part number 3HE 14220 000x TQZZA or the *VSR Release Notes*, part number 3HE 14204 000x TQZZA.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.



**Note:** This guide generically covers Release 16.0.Rx content and may contain some content that will be released in later maintenance loads. Refer to the *SR OS 16.0.Rx Software Release Notes*, part number 3HE 14220 000x TQZZA or the *VSR Release Notes*, part number 3HE 14204 000x TQZZA, for information about features supported in each load of the Release 16.0.Rx software.

## 1.2 Router Configuration Process

[Table 2](#) lists the tasks necessary to configure system security and access functions and logging features on the 7450 ESS, 7750 SR, and 7950 XRS platforms. 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 2** Configuration Process

Area	Task	Section
System security	Configure system security	<a href="#">Security Configuration Procedures</a>
	Configure RADIUS	<a href="#">RADIUS Configurations</a>
	Configure TACACS+	<a href="#">TACACS+ Configurations</a>
	Configure LDAP	<a href="#">LDAP Configurations</a>
	Configure login controls	<a href="#">Configuring Login Controls</a>
Network management	Configure SNMP elements.	<a href="#">Configuring SNMP with CLI</a>
Secure network management	Configure NETCONF elements	<a href="#">NETCONF</a>
Operational functions	Configure event and accounting logs	<a href="#">Configuring Logging with CLI</a>
Data management	Configure sFlow elements	<a href="#">sFlow</a>
Network monitoring	Configure telemetry	<a href="#">gRPC</a>
Network security	Configure TLS server and client	<a href="#">Common Configuration Tasks</a>
Equipment monitoring	Configure facility alarms	<a href="#">Configuring Logging with CLI</a>



**Note:** All features are supported on all SR OS platforms (7750 SR, 7450 ESS, and 7950 XRS) unless indicated otherwise.





---

## 2 Security

### 2.1 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.

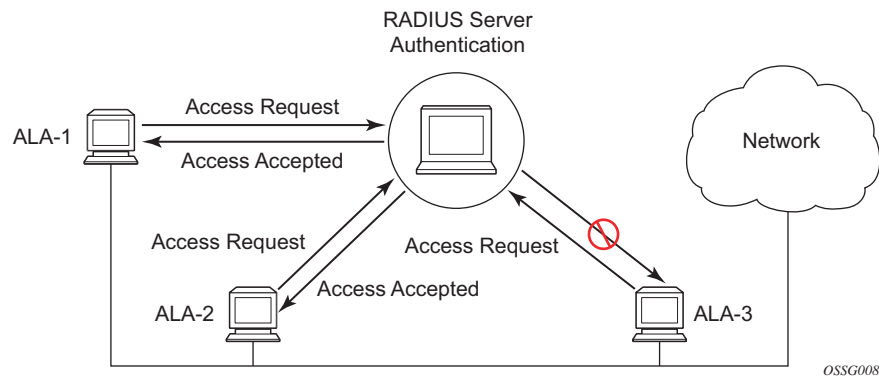
Another step, accounting, keeps track of the activity of a user who has accessed the network. The type of accounting information recorded can include a history of the commands executed, the amount of time spent in the session, the services accessed, and the data transfer size during the session. The 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

## 2.1.1 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](#)
- [RADIUS Authentication](#)
- [TACACS+ Authentication](#)
- [LDAP Authentication](#)

### **2.1.1.1 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.

### **2.1.1.2 RADIUS Authentication**

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

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

#### **2.1.1.2.1 RADIUS Server Selection**

The RADIUS server selection algorithm is used by different applications:

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

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

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

##### **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 is 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 within 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 using 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 using 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 on screen. 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 the 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 using 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 the 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.

If the idle/session attribute is not available or if the value is set to a very large number, the 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 disabled, the maximum idle-timeout (24-hours) is used for the calculation.

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

### **RADIUS Accounting**

RADIUS accounting can be used for two purposes:

- CLI command accounting
- Enhanced Subscriber Management subscriber host accounting

The RADIUS accounting application will try to send all the accounting records of a subscriber host to the same RADIUS server. If that server is down, then the records are sent to the next server, and from that moment on, the RADIUS application uses that server as the destination for accounting records for that subscriber host. Enhanced Subscriber Management applies to the 7750 SR platform.

### **RADIUS PE-Discovery**

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

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

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

## **2.1.1.3 TACACS+ Authentication**

Terminal Access Controller Access Control System (TACACS) is an authentication protocol that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a 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.



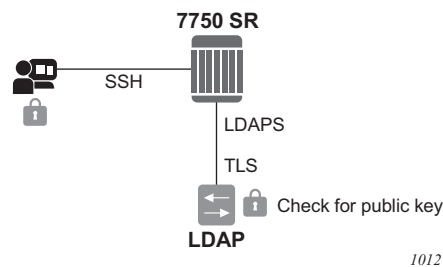
TACACS+ and RADIUS have largely replaced earlier protocols in the newer or recently updated networks. TACACS+ uses Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). TACACS+ is popular as TCP is thought to be a more reliable protocol. RADIUS combines authentication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

### 2.1.1.4 LDAP Authentication

Lightweight Directory Access Protocol (LDAP) can provide authentication, authorization, and accounting (AAA) functionality using in-band-management, and can allow users to access the full virtualized data center and networking devices. SR OS currently supports LDAP provision of a centralized authentication method with public key management. The authentication method is based on SSH public keys or keyboard authentication (username, password).

Administrators can access networking devices with one private key; public keys are usually saved locally on the SSH server. Proper key management is not feasible with locally-saved public keys on network devices or on virtual machines, as this would result in hundreds of public keys distributed on all devices. LDAPv3 provides a centralized key management system that allows for secure creation and distribution of public keys in the network. Public keys can be remotely saved on the LDAP server, which makes key management much easier, as shown in [Figure 2](#).

**Figure 2 Key Management**



The administrator starts an SSH session through an SSH client using their private key. The SSH client for the authentication method sends a signature created with the user's private key to the router. The router authenticates the signature using the user's public key and gives access to the user. To access the public key, the router looks up the public key stored on the LDAP server instead of a locally-saved key stored on the router. Communication between the router and the LDAP server should be secured with LDAP over SSL/STL (LDAPS). After successful authentication, LDAP returns a set of public keys that can be used by the router to verify the signature.

LDAP is integrated into the SR OS as an AAA protocol alongside existing AAA protocols, such as RADIUS and TACACS+. The AAA framework provides tools and mechanisms (such as method lists, server groups, and generic attribute lists) that enable an abstract and uniform interface to AAA clients, irrespective of the actual protocol used for communication with the AAA server.

The authentication functions are:

- Public key authentication — The client tries to SSH to the SR OS using public keys.  
Public keys can be stored locally or on the LDAP server and retrieved as needed to authenticate the user.
- Password authentication — Keyboard interactive  
The LDAP server can be used for user authentication using keyboard interactive, as with simple user name and password authentication.

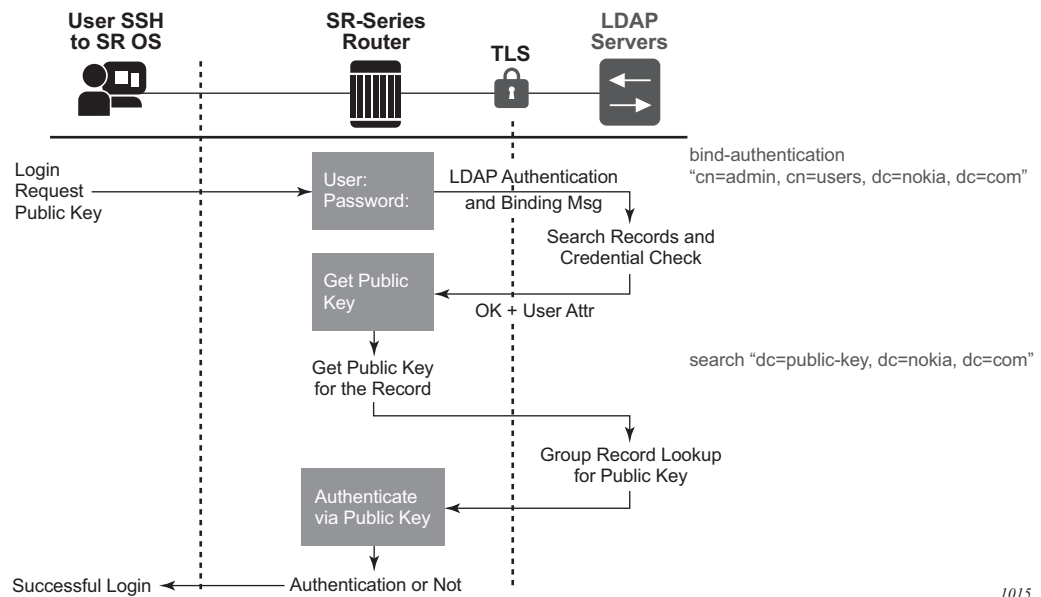
#### 2.1.1.4.1 LDAP Authentication Process

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), which—by default—are on TCP port 389 and UDP port 636 for LDAP. The SR OS then sends an operation request to the server, and the server sends responses in return, as shown in [Figure 3](#). With some exceptions, the client does not need to wait for a response before sending the next request, and the server may send the responses in any order. All information is transmitted using Basic Encoding Rules (BER).

In the SR OS, the client can request the following operations:

- StartTLS — Uses the LDAPv3 Transport Layer Security (TLS) extension for a secure connection.
- Bind — Authenticates and specify the LDAP protocol version.
- Search — Searches for and retrieve directory entries.
- Unbind — Closes the connection (not the inverse of Bind).

**Figure 3 LDAP Server and SR OS Interaction for Retrieving the Public Key**



1015

The connection between the router as the LDAP client and the LDAP server should be encrypted using TLS, as all credentials between the router and LDAP are transmitted in clear text.

#### 2.1.1.4.2 Authentication Order

SR OS supports local and LDAP public key storage, the order of which is configured using the **config>system>security>password>authentication-order** command.



**Note:** The SR OS sends available authentication methods to the client and supports public key and password authentication. If the client is configured using **public-key-authentication** then it will use the public key authentication method.

If the client chooses the public key and LDAP is first in authentication order, then the SR OS will try to authenticate using public key retrieval from the LDAP server. If the public key retrieval from LDAP server fails and **exit-on-reject** was not configured, the SR OS will try the next method (**local**) in authentication order for the public key. If the next method also fails, a user authentication fail message will be sent to the client.

If the public key retrieval from the LDAP server fails and **exit-on-reject** is configured, the SR OS will not try the next method in the authentication order. A user authentication fail message will be sent to the client. At this point, the client can be configured to only use public key authentication, or use both public key authentication followed by password authentication. If the client is configured to use password authentication, it will go through the authentication order again, (for example, it will try all the configured methods in the configured **authentication-order**) as long as **exit-on-reject** is not configured.

### Authentication Order Public Key Detail

There are two keys for public key authentication: a private key stored on the client and a public key stored on the server (local) or AAA server (LDAP). The client uses the private key to create a signature, which only the public key can authenticate. If the signature is authenticated using the public key, then the user is also authenticated and is granted access. SR OS can locally store, using CLI, as many as 32 RSA keys and 32 ECDHA keys for a single user. In total, the SR OS can load a maximum of 128 public keys in a single authentication attempt.



**Note:** The client creates a signature using a single private key, but this signature can be authenticated on the SR OS with maximum of 128 public keys in a single try. If all these public keys fail to authenticate, then a failure message will be sent to the client and the number of failed attempts will be incremented.

If the client has another private key, it can create a new signature with this new private key and attempt the authentication one more time, or switch to password authentication.

The following steps outline the procedure where the client attempts to authenticate using a public key and the authentication order is configured as **ldap**, then **local**.



**Note:** With each increment of failed attempts, the SR OS also checks the limit for lock-out. If the limit is reached, the user is locked out.

1. The SSH client opens a session and tries to authenticate the user with private-key-1 (creating signature-1 from private-key-1).
2. The SR OS checks the authentication order.
3. The SR OS loads public keys for the user, as follows.
  - a. If **exit-on-reject** is not configured, the SR OS loads all public keys from the LDAP server and all public keys from the locally-saved location.

- b. If **exit-on-reject** is configured, the SR OS only loads all public keys from the LDAP server and not from the locally-saved location.
4. The SR OS compares received client signature-1 with signature calculated from loaded public keys and attempts to find a match.
  - a. If a match is found, the user is authenticated. The procedure ends.
  - b. If no match is found, authentication fails and the SSH client is informed. The LDAP server waits for the SSH client's reaction.
5. The SSH client reacts in one of several ways.
  - a. The connection is closed.
  - b. The password authentication method is continued. In this case, on the SR OS, the number of failed authentication attempts is not incremented.
  - c. The next public key is continued, as follows.
    - i. If it is not 21st received public key, return to step 3.
    - ii. If it is the 21st received public key, the number of failed authentication attempts is incremented and the connection is closed.

#### 2.1.1.4.3 LDAP Authentication Using a Password

In addition to public key authentication, the SR OS supports password (keyboard) authentication using the LDAP server.



**Note:** TLS provides the encryption for password authentication.

In the following example, the client attempts to authenticate using a password and only **ldap** is configured in the authentication order.

1. The client uses telnet or SSH to reach the SR OS.
2. The SR OS retrieves the user name and password (in plain text).
3. The SR OS performs a bind operation to the LDAP server using the **config>system>security>ldap>server>bind-operation** command to set the *root-dn* and *password* variables.
4. The SR OS performs a search operation for the username on LDAP server.
  - a. If the user name is found, LDAP sends user\_distinguished\_name to the router.
  - b. If the user name is not found, the authentication fails. The attempt and failed attempt counters will be incremented.

5. The SR OS performs a bind operation to LDAP with `user_distinguished_name` and the password from step 2.
6. The LDAP server checks the password.
  - a. If the password is correct, the bind operation succeeds. The failed attempt and successful attempt counters are incremented.
  - b. If the password is incorrect, bind is unsuccessful and authentication fails. The attempt and failed attempt counters are incremented.
7. The SR OS sends a message to unbind from the LDAP server.

#### 2.1.1.4.4 Timeout and Retry Configuration for the LDAP Server

The **retry** value is the maximum number of connection attempts that the SR OS can make to reach the current LDAP server before attempting the next server. For example, if the value is set to the default of 3, the SR OS will try to establish the connection to current server three times before attempting to establish a connection to the next server.

The **timeout** value is the number of seconds that the SR OS will wait for a response from the server with which it is attempting to establish a connection. If the server does not reply within the specified timeout value, the SR OS increments the **retry** counter by one. The SR OS attempts to establish the connection to the current server up to the configured **retry** value before moving to the next configured server.

#### 2.1.1.4.5 TLS Behavior and LDAP

RFC 4511 section 4.14.1 states, “A client requests TLS establishment by transmitting a StartTLS request message to the server” and “The client MUST NOT send any LDAP PDUs at this LDAP message layer following this request until it receives a StartTLS Extended response”. As such, if an LDAP has a TLS profile configured and the TLS is in an operationally down state, no LDAP packets will be transmitted if TLS negotiation has not been completed, including when the TLS profile is shut down.

#### 2.1.1.4.6 LDAP Health Check

The health check for LDAP is configured under **config>system>security>password**.

The **health-check** function, which can be disabled, is available for operator management. The health check polls the server at a specified interval (the default is 30 seconds). The SR OS health check attempts to establish a TCP connection to the LDAP server. The TCP connection is closed by an LDAP unbind message.

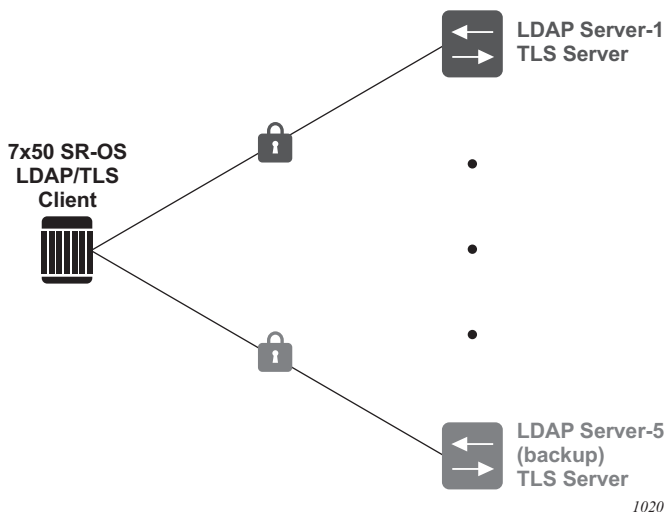
#### 2.1.1.4.7 LDAP Redundancy and TLS

LDAP supports up to five redundant (backup) servers. Depending on the configuration of **timeout** and **retry** values, if an LDAP server is found to be out of service or operationally down, the SR OS will switch to the redundant servers. The SR OS will try the next LDAP server in the server list by choosing the next largest configured server index.

LDAP servers can use the same TLS profile or can have their own TLS profile. Each TLS profile can have a different configuration of **trust-anchor**, **cipher-list** and **cert-profile**. For security reasons, the LDAP server could be in different geographical areas and, as such, each will be assigned its own server certificate and trust anchor. The TLS profile design allows users to mix and match all components.

Redundant LDAP servers are shown in [Figure 4](#).

**Figure 4** LDAP and TLS Redundancy



1020

## 2.1.2 Authorization

The SR OS supports 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](#)
- [RADIUS Authorization](#)
- [TACACS+ Authorization](#)

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 \(VSAs\)](#).

### 2.1.2.1 Local Authorization

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

By default, local authorization is enabled. Local authorization is disabled only when a different remote authorization method is configured, such as TACACS+ or RADIUS authorization and local is removed from the authorization order.

You must configure profile and user access information locally.

### 2.1.2.2 RADIUS Authorization

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

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 3 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 3 Supported Authorization Configurations**

	Router	RADIUS Supplied Profile
Router configured user	Supported	Not Supported
RADIUS server configured user	Supported	Supported
TACACS+ server configured user	Supported	Not Supported

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

### 2.1.2.3 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, 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 **user-template tacplus\_default** 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 the 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.

### 2.1.2.3.1 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, the 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
```

## 2.1.2.4 Authorization Profiles for Different Interfaces

Authorization profiles can be configured in any format including classic CLI and MD-CLI. Depending on the configuration, a match might be hit.

Each entry in a profile can be formatted for classic CLI or MD-CLI. Nokia recommends creating separate profiles for each interface type. For example, a profile for classic CLI and a different profile for MD-CLI.

[Table 4](#) shows authorization and match hit based on the entry format configuration. This is true whether authorization is done using local user profiles or using an AAA server like TACACS+ or RADIUS.

**Table 4** Authorization and Match Hit Based on Entry Format

Profile Entry Format	NETCONF	gRPC	MD-CLI	Classic CLI
Classic CLI	Maybe	Maybe	Maybe	Yes
MD-CLI	Yes	Yes	Yes	Maybe

## 2.1.2.5 Authorization Support

Table 5 shows authorization support using a local profile or an AAA server.

**Table 5** Authorization Support

	MD-CLI	NETCONF	gRPC	Classic CLI
LDAP	N/A	N/A	N/A	N/A
TACACS+	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
Local	Yes	Yes	Yes	Yes

### 2.1.2.5.1 Default User and Admin Profiles

A default profile is made for all interface types: classic CLI and MD-CLI. There is an admin group and default group for authorization. An admin user must be part of the admin group automatically. In classic CLI, other users will be in the default group unless specifically moved from that group by the admin. In MD-CLI, users must be added to the default group by the administrator.

### 2.1.2.5.2 Authorization Support for Groups

Authorization for groups is done explicitly by creating an entry for that group configuration.

For example, to deny an interface to config and config>groups create an entry for each one.

```
Entry 10
  Match "configure router base interface"
  Action deny
Entry 20
  Match "configure group router base interface"
  Action deny
```

---

## 2.1.3 Accounting

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

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

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

### 2.1.3.1 RADIUS Accounting

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

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

### 2.1.3.2 TACACS+ Accounting

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

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

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

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

## 2.2 Security Controls

You can configure routers to use RADIUS, TACACS+, and local authentication to validate users requesting access to the network. The order in which password authentication is processed among RADIUS, TACACS+ and local passwords can be specifically configured. 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. The security methods capabilities are listed in [Table 6](#).

**Table 6** 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 <b>config log</b> command.			

### 2.2.1 When a Server Does Not Respond

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

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

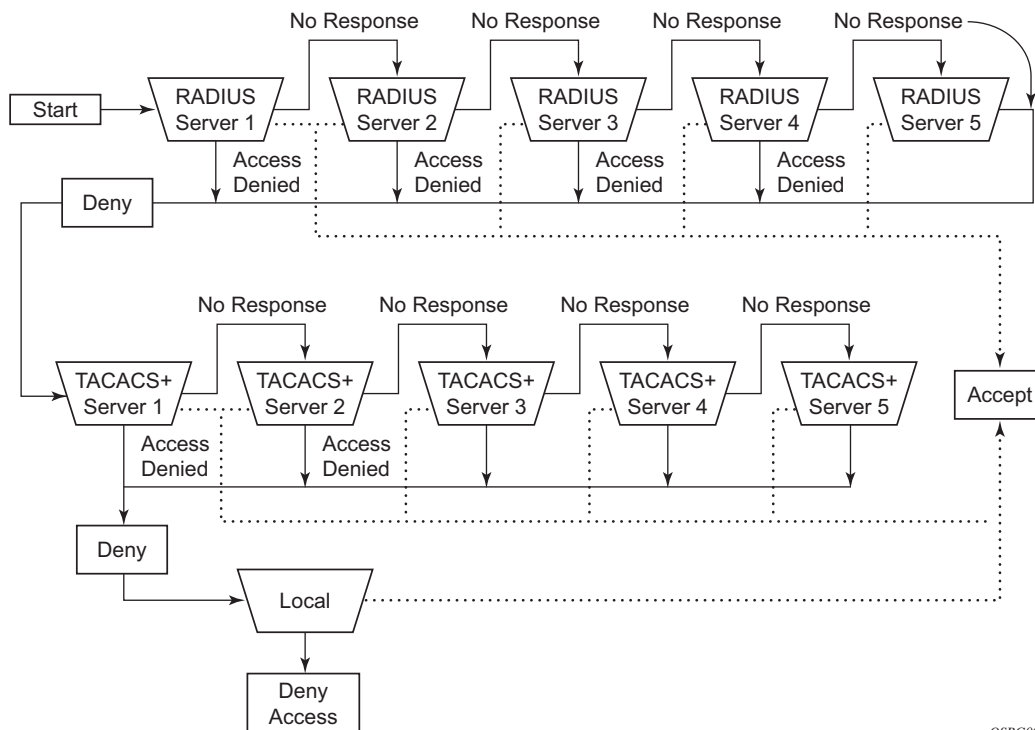
The servers are accessed in order from lowest to highest specified index (from 1 to 5) for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received, implying a lower indexed server is not available. If a response from the server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

## 2.2.2 Access Request Flow

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

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

**Figure 5 Security Flow**



OSRG009



## 2.3 Control and Management Traffic Protection

SR OS routers support an extensive set of configurable mechanisms to protect the CPU from being flooded with control or management traffic.

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

- In-band traffic extracted from the line cards to the CPM:
  - Line card features:
    - ACLs filters: IPv4, IPv6, and MAC
    - Anti-spoofing, uRPF
    - Distributed CPU protection
  - CPM features:
    - CPM Filters: IPv4, IPv6, and MAC
    - Centralized CPU Protection
    - Per-peer queues, protocol queues, CPM queues
- Out-band and in-band traffic: Management access filters

### 2.3.1 CPM Filters

CPM filters are hardware-based filters used to restrict traffic from the line cards directed to the control processor. This filtering is performed by the Fast Path (FP) network processor and it uses no resources on the main CPU.

CPM filters filter traffic is extracted from the data plane and sent to the CPM for processing. Packets from all network and access ports is filtered. Packets originating from a management Ethernet port can be filtered using management access filters. See [Management Access Filter](#) for more information.

#### 2.3.1.1 CPM Filter Packet Match

Three different CPM filter policies can be configured: **ip-filter**, **ipv6-filter**, and **mac-filter**.

CPM Filter packet match rules:

- Each CPM filter policy is an ordered list of entries. Entries must be sequenced correctly from the most to the least explicit.
- If multiple match criteria are specified in a single CPM filter policy entry, all criteria must be met for the packet to be considered a match against that policy entry (logical AND).
- Any match criteria not explicitly defined is ignored during a match.
- A CPM filter policy entry defined without any match criteria is inactive.
- A CPM filter policy entry with match criteria defined, but no action configured, inherits the default action defined at the **cpm-filter** level.
- The **cpm-filter default-action** applies to IPv4, IPv6, or MAC CPM filters that are in a **no shutdown** state.
- When **mac-filter** and **ip-filter/ipv6-filter** are applied to a specific packet, the **mac-filter** is applied first.

### 2.3.1.2 CPM IPv4 and IPv6 Filter Entry Match Criteria

The supported IPv4 and IPv6 match criteria are shown in the following tables.

[Table 7](#) lists the basic Layer 3 match criteria.

**Table 7 Basic Layer 3 Match Criteria**

Criteria	Description
<b>dscp</b>	Matches the specified DSCP value against the DSCP/Traffic Class field in the IPv4 or IPv6 packet header.
<b>src-ip/dst-ip</b>	Matches the specified source/destination IPv4/IPv6 address prefix/mask against the source/destination IPv4/IPv6 address field in the IP packet header. Optionally, operators can match a list of IP addresses defined in <b>filter match-list ip-prefix-list</b> or <b>match-list ipv6-prefix-list</b> . The <b>prefix-list</b> can be defined statically or using the <b>apply-path</b> command to automatically populate using configured BGP peers defined in the base router or VPRN services. Refer to the “Match List for Filter Policies” section in the <i>Router Configuration Guide</i> for more details on filter <b>match-list</b> configuration and capabilities.
<b>fragment</b>	For IPv4, match against the MF bit or Fragment Offset field to determine if the packet is a fragment. For IPv6 match against the next-header field or Fragment Extension Header value to determine whether the packet is a fragment. Up to six extension headers are matched against to find the Fragmentation Extension Header.

[Table 8](#) lists the IPv4 options match criteria.

**Table 8 IPv4 Options Match Criteria**

Criteria	Description
<b>ip-option</b>	Matches the specified option value in the first option of the IPv4 packet. Optionally, operators can configure a mask to be used in a match.
<b>option-present</b>	Matches the presence of IP options in the IPv4 packet. Padding and EOOL are also considered as IP options. Up to six IP options are matched against.
<b>multiple-option</b>	Matches the presence of multiple IP options in the IPv4 packet.

[Table 9](#) lists the IPv6 next-header match criteria.

**Table 9 IPv6 Next-header Match Criteria**

Criteria	Description
<b>hop-by-hop-opt</b>	Matches for the presence of hop-by-hop options extension header in the IPv6 packet. This match criterion is supported on ingress only. Up to six extension headers are matched against.

[Table 10](#) lists the upper-layer protocol match criteria.

**Table 10 Upper-layer Protocol Match Criteria**

Criteria	Description
<b>next-header</b>	Matches the specified upper-layer protocol (such as TCP or UDP) against the next-header field of the IPv6 packet header. "*" can be used to specify TCP or UDP upper-layer protocol match (logical OR). Next-header matching also allows matching on the presence of a subset of IPv6 extension headers. See the CLI section for information on which extension header match is supported.
<b>protocol</b>	Matches the specified protocol against the Protocol field in the IPv4 packet header (for example, TCP, UDP, or IGMP) of the outer IPv4. "*" can be used to specify TCP or UDP upper-layer protocol match (logical OR).
<b>icmp-code</b>	Matches the specified value against the Code field of the ICMP/ICMPv6 header of the packet. This match is supported only for entries that also define protocol/next-header match for ICMP/ICMPv6 protocol.

**Table 10 Upper-layer Protocol Match Criteria (Continued)**

Criteria	Description
<b>icmp-type</b>	Matches the specified value against the Type field of the ICMP or ICMPv6 header of the packet. This match is supported only for entries that also define protocol/next-header match for "ICMP" or "ICMPv6" protocol.
<b>src-port/dst-port/port</b>	Matches the specified port value (with or without mask), port list, or port range against the Source Port Number/Destination Port Number of the UDP/TCP packet header. An option to match either source or destination port or both (logical OR) using a single filter policy entry is supported by using a directionless <b>port</b> command. Source/destination match is supported only for entries that also define protocol/next-header match for "TCP", "UDP" or "TCP or UDP" protocols. A non-initial fragment will not match an entry with non-zero port criteria specified.
<b>tcp-ack/tcp-syn</b>	Matches the presence or absence of the TCP flags in the TCP header of the packet. This match criteria also requires defining the protocol/next-header match as "TCP".

[Table 11](#) lists the router instance match criteria.

**Table 11 Router Instance Match Criteria**

Criteria	Description
<b>router</b>	Matches the router instance packets that are ingressing from for this filter entry.

### 2.3.1.3 CPM MAC Filter Entry Match Criteria

The MAC match criteria are evaluated against the Ethernet header of the Ethernet frame.

[Table 12](#) lists the router instance match criteria.

**Table 12 Router Instance Match Criteria**

Criteria	Description
<b>frame-type</b>	The filter matches a specific type of frame format. For example, configuring frame-type ethernet_II matches only Ethernet-II frames.

**Table 12 Router Instance Match Criteria (Continued)**

Criteria	Description
<b>src-mac</b>	Matches the specified source MAC address frames. Optionally, operators can configure a mask to be used in a match.
<b>dst-mac</b>	Matches the specified destination MAC address frames. Optionally, operators can configure a mask to be used in a match.
<b>etype</b>	Matches the specified Ethernet II frames. The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame.
<b>ssap</b>	Matches the specified frames with a source access point on the network node designated in the source field of the packet. Optionally, operators can configure a mask to be used in a match.
<b>dsap</b>	Matches the specified frames with a destination access point on the network node designated in the destination field of the packet. Optionally, operators can configure a mask to be used in a match.
<b>cfm-opcode</b>	Matches the specified packet with the specified <b>cfm-opcode</b> .

### 2.3.1.4 CPM Filter Policy Action

The two main CPM filter actions allow the option to accept or drop traffic.

Optionally, traffic can be sent to a user-configured hardware queue using a CPM filter. Nokia recommends this primarily for temporary debug or attack investigation activities.

### 2.3.1.5 CPM Filter Policy Statistics and Logging

Refer to the "Filter Policy Logging" and "Filter Policy" sections in the *Router Configuration Guide*.

### 2.3.1.6 CPM Filter: Protocols and Ports

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

[Table 13](#) identifies which ports are used by which applications in SR OS. The source port and destination port reflect the CPM filter entry configuration for traffic ingressing the router and sent to the CPM.

**Table 13      Protocols and Ports**

Src Port Number	Dst Port Number	IP Protocol	Application	Description	Accessible using Out of Band	Accessible using Network
	20	TCP	FTP	FTP Server Data. Active FTP Client.	Yes	Yes
	21	TCP	FTP	FTP Server Control	Yes	Yes
20		TCP	FTP	FTP Client Data	Yes	Yes
21		TCP	FTP	FTP Client Control	Yes	Yes
	22	TCP	SSH	SSH Server. Terminated TCP session.	Yes	Yes
22		TCP	SSH	SSH Client. Responses for initiated TCP sessions.	Yes	Yes
	23	TCP	TELNET	TELNET server	Yes	Yes
49		TCP	TACACS	TACACS client. Responses for initiated sessions.	Yes	Yes
53		UDP	DNS	DNS client	No	Yes
67	67	UDP	DHCPv4	DHCPv4: Relay agent to server, server to relay agent, and relay agent to relay agent	No	Yes
68	67	UDP	DHCPv4	DHCPv4: Client to relay agent / server	No	Yes
67	68	UDP	DHCPv4	DHCPv4: relay agent / server to client	No	Yes
	123	UDP	NTP	NTP server	Yes	Yes
123		UDP	NTP	NTP client	Yes	Yes
	161	UDP	SNMP	SNMP server: SET and GET commands	Yes	Yes
	179	TCP	BGP	BGP: server terminated TCP sessions	No	Yes
179			BGP	BGP: client responses for initiated TCP session	No	Yes

**Table 13 Protocols and Ports (Continued)**

Src Port Number	Dst Port Number	IP Protocol	Application	Description	Accessible using Out of Band	Accessible using Network
	319	UDP	PTP	1588 PTP event	No	Yes
	320	UDP	PTP	1588 PTP general	No	Yes
389		TCP	LDAP	LDAP client (non TLS)	No	Yes
	520	UDP	RIP	RIP	No	Yes
546	547	UDP	DHCPv6	DHCPv6 - Client to Server / Relay Agent	No	Yes
547	547	UDP	DHCPv6	DHCPv6 - server to relay agent, relay agent to server, and relay agent to relay agent	No	Yes
	639	UDP	PIM	MSDP: multicast source discovery protocol	No	Yes
636		TCP	LDAPS	LDAP client over TLS	No	Yes
	646	UDP	LDP	LDP Hello adjacency	No	Yes
	646	TCP	LDP	LDP/T-LDP: terminated TCP sessions	No	Yes
646		TCP	LDP	LDP/T-LDP: responses for initiated TCP sessions	No	Yes
	701	UDP	LMP	Link management protocol	No	Yes
	830	TCP	NETCONF	NETCONF	No	Yes
	862	TCP	TWAMP	TWAMP control: terminated TCP session	No	Yes
	ANY	UDP	TWAMP	TWAMP test	No	Yes
	862, 64344-64373	UDP	TWAMP	TWAMP light (per-router instance)	No	Yes
	1025	UDP	MC-LAG-APS-EP-IPsec	Multi Chassis: LAG, APS (Automation Protection Switching), End Point, IPsec (MIMP), AARP	No	Yes
	1491	TCP	SNMP Streaming	SNMP streaming server	Yes	Yes

**Table 13**      **Protocols and Ports (Continued)**

Src Port Number	Dst Port Number	IP Protocol	Application	Description	Accessible using Out of Band	Accessible using Network
	1645	UDP	Radius Proxy	Radius proxy authentication	No	Yes
	1646	UDP	Radius Proxy	Radius proxy accounting	No	Yes
	1701	UDP	L2TP	L2TP server	No	Yes
1812		UDP	RADIUS	RADIUS authentication	Yes	Yes
1813		UDP	RADIUS	RADIUS accounting	Yes	Yes
	2000	UDP	WPP	Web portal authentication protocol	No	Yes
	2123	UDP	GTP	GTP control plane	No	Yes
2123		UDP	GTP	GTP control plane	No	Yes
	2152	UDP	GTP	GTP user plane	No	Yes
2152		UDP	GTP	GTP user plane	No	Yes
	3232	UDP	PIM	PIM MDT	No	Yes
	3503	UDP	OAM	LSP ping	No	Yes
3868		UDP	DIAMETER	Diameter	Yes	Yes
	3784	UDP	BFD	BFD Control 1 hop BFD and BFD over MPLS LSP	No	Yes
	3785	UDP	BFD	BFD echo	No	Yes
	3799	UDP	RADIUS	Radius Dynamic Authorization (CoA / DM)	Yes	Yes
	4189	TCP	CPEP	PCEP - Path Computation Element Protocol	Yes	Yes
	4739	UDP	NAT	NAT debug	No	Yes
	4784	UDP	BFD	BFD control multi-hop	No	Yes
	5351	UDP	NAT	PCP NAT port mapping protocol	No	Yes
	6068	TCP	ANCP	ANCP - terminated TCP session	No	Yes



**Table 13 Protocols and Ports (Continued)**

Src Port Number	Dst Port Number	IP Protocol	Application	Description	Accessible using Out of Band	Accessible using Network
	6653	TCP	OpenFlow	OpenFlow - terminated TCP sessions	No	Yes
	6784	UDP	BFD	uBFD	No	Yes
	33408-33535	UDP	OAM	OAM Traceroute	No	Yes
	45067	TCP	MCS	Multi-chassis synchronization - Terminated TCP Session ( <b>mcs, mc-ring, mc-ipsec</b> )	No	Yes
45067		TCP	MCS	Multi-chassis synchronization - Responses for initiated TCP session ( <b>mcs, mc-ring, mc-ipsec</b> )	No	Yes
	49151	UDP	L2TP	L2TP	No	Yes
	57400	TCP	gRPC	gRPC	No	Yes
N/A	N/A	GRE	GRE	GRE	No	Yes
N/A	N/A	ICMP	ICMP	ICMP	No	Yes
N/A	N/A	IGMP	IGMP	IGMP	No	Yes
N/A	N/A	OSPF	OSPF	OSPF	No	Yes
N/A	N/A	PIM	PIM	PIM	No	Yes
N/A	N/A	RSVP	RSVP	RSVP	No	Yes
N/A	N/A	VRRP	VRRP	VRRP	No	Yes
pki-server-port or 80/8080	any	TCP	PKI	CMPv2 (Certificate Management Protocol v2) client - Responses for initiated TCP session	No	Yes
pki-server-port	any	TCP	PKI	OCSP (Online Certificate Status Protocol) client - Responses for initiated TCP session	No	Yes
pki-server-port or 80/8080	any	TCP	PKI	Auto CRL (Certificate Revocation List) update (client) - Responses for initiated TCP session	Yes	Yes

---

## 2.3.2 CPM Per-Peer Queuing

Per-peer queuing provides isolation between peers by allocating hardware queues on a per-peer basis for the following TCP-based protocols: BGP, T-LDP, LDP, MSDP, Telnet, and SSH.

This mechanism guarantees fair and non-blocking access to shared CPU resources across all peers. For example, this ensures that an LDP-based DoS attack from a specific peer is mitigated and compartmentalized and not all CPU resources are dedicated to the overwhelming control traffic sent by that specific peer.

The **per-peer-queuing** command ensures that service levels would not be (or only partially be) impacted in case of an attack towards BGP, T-LDP, LDP, MSDP, Telnet, or SSH. SSH and Telnet supports per-peer queuing when the **login-control ttl-security** command is enabled.

## 2.3.3 Centralized CPU Protection

SR OS CPU protection is a centralized rate-limiting function that operates on the CPM to limit traffic destined to the CPU. The term “centralized CPU protection” is referred to as “CPU protection” in this guide and in the CLI to differentiate it from “Distributed CPU Protection”.

CPU protection provides interface isolation by rate limiting the total amount of traffic extracted to the CPM per port, interface, or SAP in hardware using a combination of limits configurable at the CPU protection system level or as CPU protection policies assigned to access or network interfaces.

The following limits are configurable at the CPU protection system level:

- **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, 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.

The following limits are configurable independently for access or network interfaces using a dedicated CPU protection policy:

- **overall-rate** — Applies to all control traffic destined to the CPM (all sources) received on an interface 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* tuple for IP source 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 an interface where the policy is applied. This is a per-interface limit. Control traffic received above this rate will be marked as discard eligible (such as, out-profile/low-priority/yellow) and is more likely to be discarded if there is contention for CPU resources.

There are two default CPU protection policies for access and network interfaces.

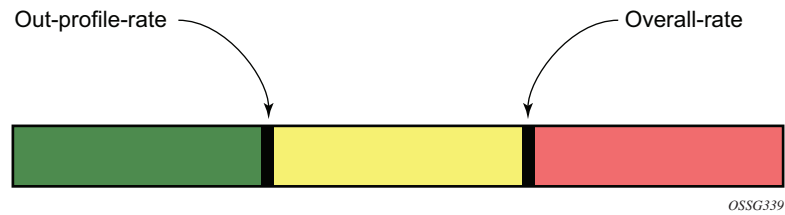
Policy 254:

- 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 queuing towards the CPU
- overall-rate = max
- per-source-rate = max
- out-profile-rate = 3000

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 CPU protection policy called **out-profile-rate** maps to the boundary between the green (accept) and yellow (mark as discard eligible/low priority) regions. The **overall-rate** command marks the boundary between the yellow and red (drop) regions point for the associated policy ([Figure 6](#)).

**Figure 6 Profile Marking**

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/low priority in the case of the **out-profile-rate**) and traffic on the interface is affected.

This rate limit protects all the other interfaces and ensures that a violation from one interface does not affect the rest of the system.

CPU protection is not supported on 7750 SR-1, 7750 SR-e, and 7750 SR-a.

### 2.3.3.1 Protocol Protection

Protocol protection allows traffic to be discarded for protocols not configured on the router. This helps mitigate DoS attacks by filtering invalid control traffic before it reaches the CPU. This is a feature of CPU Protection and can be enabled or disabled for the entire system.

When using **protocol-protection**, the system automatically maintains a per-interface list of configured protocols. For example, if an interface does not have IS-IS configured, then protocol protection will discard any IS-IS packets received on that interface. Other protocols, such as L2TP, are controlled by **protocol-protection** at the VPRN service level.

Protocols controlled by the **protocol-protection** mechanism include:

- GTP
- IGMP
- IS-IS
- MLD
- L2TP control
- OSPFv2
- OSPFv3

- PPPoE
- PIM
- RIP

The following protocols are protected independently from Protocol Protection:

- **per-peer-queuing** protects BGP, LDP, T-LDP, MSDP, Telnet and SSH
- BFD control packets are dropped if BFD is not configured on a specific interface

### 2.3.3.2 CPU Protection Extensions for ETH-CFM

CPU protection supports 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 to 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 as listed in [Table 14](#), with a range of five (5) to seven (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 created.

**Table 14** 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 or binding within a service for these rates to take effect. This means the rate is on a per-SAP or per-binding basis. Only one policy may be applied to each SAP or 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 or 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 or binding by configuring **eth-cfm-monitoring** which does not have an MP. In this case, although these entries are enforced, no packets are redirect to the CPU.

By default, rates are applied on a per-peer basis. This means each individual peer is subject to the rate. Use the **aggregate** option to apply the rate to 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 not required, making the aggregate function more appealing.

The **eth-cfm-monitoring** and **mac-monitoring** commands are mutually exclusive and cannot be configured on the same SAP or binding. The **mac-monitoring** command is used in combination with the traditional CPU protection and is not specific to ETH-CFM rate limiting feature described here.

When an MP is configured on a SAP or binding within a service which allows an external source to communicate with that MP, for example a User to Network Interface (UNI), **eth-cfm-monitoring** with the **aggregate** option should be configured on all SAPs or 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 an 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
```

The centralized CPU protection features are supported on the following platforms:

- 7750 SR-7/SR-12
- 7450 ESS-7/ESS-12
- 7950 XRS

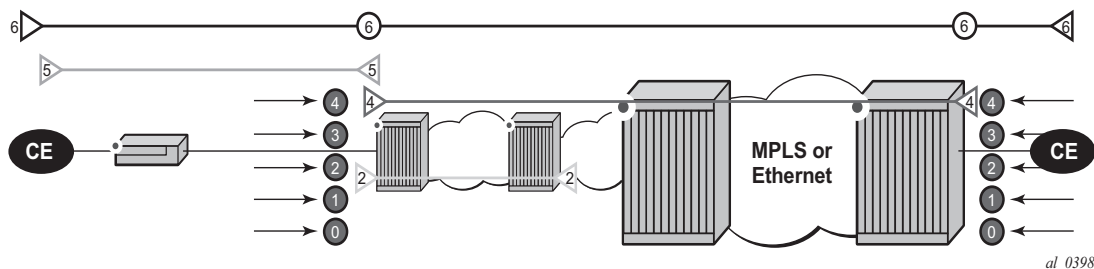
### 2.3.3.3 ETH-CFM Ingress Squelching

CPU protection provides a granular method to control which ETH-CFM packets are processed. As indicated in [CPU Protection Extensions for ETH-CFM](#), a unique rate can be applied to ETH-CFM packets classifying on specific MD-level and a specific OpCode and applied to both ingress (down MEP and ingress MIP) and egress (up MEP and egress MIP) extraction. This function is to protect the CPU on extraction when a Management Point (MP) is configured.

It is also important to protect the ETH-CFM architecture deployed in the service provider network. This protection scheme 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 drops all ETH-CFM packets at or below the configured MD-level. The ETH-CFM squelch feature is supported at ingress only.

Figure 7 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 each level 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 7** ETH-CFM Hierarchical Model



Squelching configuration uses a single MD-level (0 to 7) to silently drop all ETH-CFM packets matching the SAP or binding delimited configuration at or below the specified MD-level. In Figure 7, 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 means that any existing MEP or MIP processing ingress CFM packets on a SAP or 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 processed followed by CPU protection for ETH-CFM.

MPs configured to support primary VLANs 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 15](#). 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 15 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 also appears in the output of 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
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 10.1.1.1         0 1 2 3 4
=====
```

---

## 2.3.4 Distributed CPU Protection (DCP)

Distributed CPU Protection (DCP) is a rate-limiting function distributed to the line cards to rate-limit traffic extracted from the data path and sent to the CPM. DCP is performed in hardware and provides per-interface, access or network, and per-protocol granular rate-limit control.

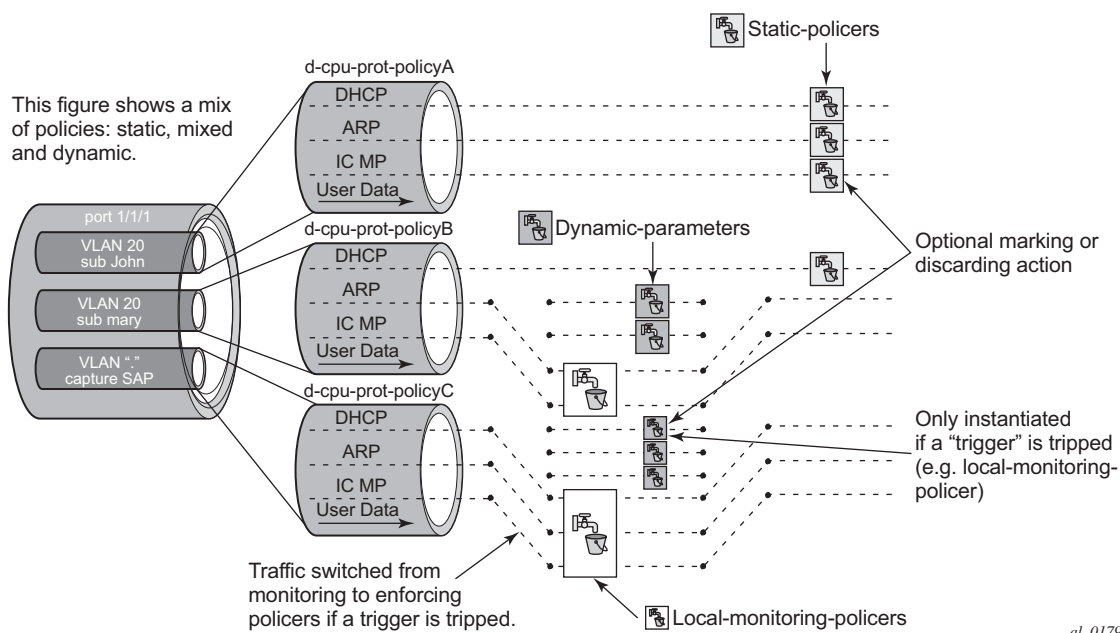
DCP rate limiting is configured using policies that are applied to objects (for example, SAPs).

The basic types of policers in DCP are:

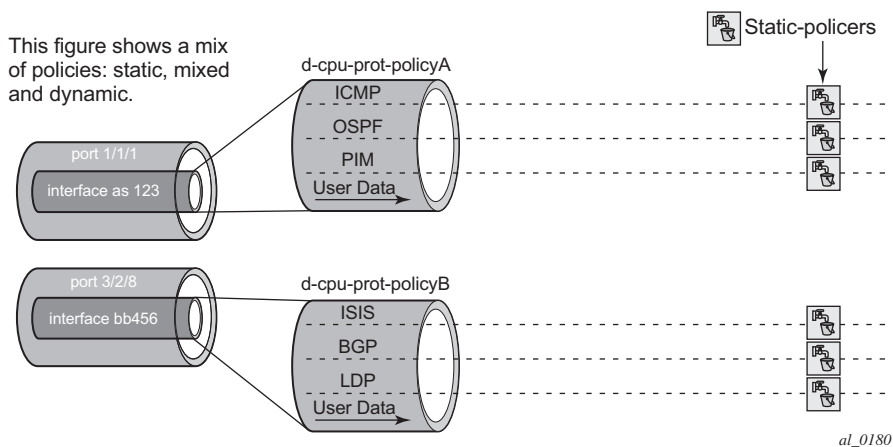
- Enforcement policers — An instance of a policer that is policing a flow of packets comprised of a single (or small set of) protocols arriving on a single object (for example, SAP). Enforcement policers perform a configurable action (for example, discard) on packets that exceed configured rate parameters. 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 nonconformance 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 8 Per SAP Per-protocol Static Rate Limiting with DCP**



**Figure 9 Per Network Interface Per-protocol Static Rate Limiting with DCP**



---

### 2.3.4.1 Applicability of Distributed CPU Protection

The system assigns a default Distributed CPU Protection (DCP) policy to newly-created access and network interfaces. Originally, these policies, “\_default-access-policy” and “\_default-network-policy”, are created empty and are modifiable by the operator. Additional DCP policies can be created for interfaces requiring a dedicated configuration.

If DCP functionality is not required on a given access or network interface, then an empty DCP policy can be created and explicitly assigned to the interface.

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

- most types of SAPs, including capture SAPs, SAPs on pseudowires, B-VPLS SAPs and VPLS template SAPs, but are not applicable to Epipe template SAPs and video ISA 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 DCP (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 and interface CPU protection can be employed to rate limit or mark this traffic.

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 through 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 Layer 3-interface bound to them (R-VPLS), may have protocols such as OSPF, ARP, configured in the policy.

---

### 2.3.4.2 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 subscribers 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 through:

- 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

### 2.3.4.3 DCP Policer Resource Management

The policer instances are a limited hardware 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 or 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 or global policer pool on the card or 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 or FP, then the object will not be 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 not be created.

Dynamic enforcement policers are allocated as needed (when the local monitor detects nonconformance) 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 FP (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 or 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.

#### **2.3.4.4 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 not 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 kb/s 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:** 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 is trusted, and using the “all-unspecified” protocol is not required, then avoid referencing this protocol in the policy configuration.
- If a protocol is trusted, but the all-unspecified bucket is required, then there are two options:
  - avoid creating a protocol 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)
  - create this protocol and configure it to bypass

## 2.3.5 Classification-Based Priority for Extracted Protocol Traffic

The SR OS supports a set of mechanisms to protect the router control and management planes from various types of attacks, floods, and misconfigurations. Many of the mechanisms operate by default with no need for operator configuration or intervention.

One class of mechanisms employed on the router to protect against floods of control traffic involves identifying potentially harmful or malicious traffic through the use of rate measurements. Centralized CPU protection protects and isolates interfaces from each other by default by treating unexpectedly high rate control traffic on an interface as lower priority (to be discarded if the control plane experiences congestion). Distributed CPU protection can protect and isolate at a per-protocol, per-interface granularity through configured rate profiles. These rate-based protection mechanisms make no assumptions about the contents of the packets and can be used when nothing about the packets can be trusted (for example, DSCP or source IP address, which can be spoofed).

The SR OS also supports an alternative to rate-based mechanisms for cases where the packet headers can be trusted to differentiate between good and bad control traffic. A configurable prioritization scheme can be enabled (using the **init-extract-prio-mode l3-classify** command) on a per-FP basis to initialize the drop priority of all Layer 3 extracted control traffic based on the QoS classification of the packets. This is useful, for example, in networks where the DSCP and EXP markings can be trusted as the primary method to distinguish, protect, and isolate good terminating protocol traffic from unknown or potentially harmful protocol traffic instead of using the rate-based distributed CPU protection and centralized CPU protection traffic marking/coloring mechanisms (for example, **out-profile-rate** and **exceed-action low-priority**).

The operational guidelines for deploying classification-based priority for extracted control traffic are as follows.

- Centralized CPU protection should be effectively disabled for all interfaces/SAPs on FPs configured in **l3-classify** mode by changing some CPU protection policy parameters from their default values. This is required so that centralized CPU protection does not re-mark good control traffic (traffic that was initially classified as high priority) as low priority if a flood attack occurs on the same interface. Effectively disabling centralized CPU protection can be done by ensuring that:
  - a rate value of **max** is configured for **port-overall-rate** (**max** is the default value for **port-overall-rate**)



- all objects (interfaces, MSAP policies, and SAPs) that can be assigned a CPU protection policy are referencing a policy that sets the **out-profile-rate** to **max** and the **overall-rate** to **max** (this can be done in the two default CPU protection policies if all FPs in the system are in **I3-classify** mode)
- DCP can be used in conjunction with **I3-classify** mode, but care must be taken to prevent DCP from acting on protocols where the operator wants to use QoS classification (such as DSCP or EXP) to differentiate between good and bad Layer 3 packets. On an FP with **I3-classify** mode, DCP should be configured so that BGP, LDP, and other protocols do not have their initial drop priority (color) overwritten by DCP if the QoS classification of these protocols is trusted. This can be achieved by using **exceed-action none** for those protocols in a DCP policy. For other protocols where QoS classification cannot be used to distinguish between good and bad extracted packets, DCP can be used to color the packets with a drop priority based on a configured rate.
- If any LAG member is on an FP in **I3-classify** mode, all FPs that host the other members of that LAG should also be in **I3-classify** mode.
- The QoS classification rules that are used on interfaces/SAPs on FPs in **I3-classify** mode should be configured to differentiate between good and bad control traffic. The default network ingress QoS policies do differentiate (for example, based on DSCP), but the default access ingress QoS policies do not.

The **I3-classify** mode for extracted control traffic is supported on the 7750 SR and 7950 XRS.

## 2.3.6 TTL Security

This SR OS routers TTL security feature evaluates the incoming TTL value against a configured TTL for BGP peers, LDP peers, SSH, and Telnet in hardware. If the incoming TTL value is less than the configured TTL value, the packets are discarded and a log is generated preventing attackers generating spoof traffic with larger number of hops than expected.

The TTL value is configurable on a per-peer basis for BGP and LDP and configurable at the system level for SSH and Telnet.

The TTL security mechanism was originally designed to protect the BGP infrastructure from CPU utilization-based attacks. It is derived on the fact that the vast majority of ISP eBGP peerings are established between adjacent routers. Since TTL spoofing cannot be performed, a mechanism based on an expected TTL value provides a simple and robust defense from infrastructure attacks based on forged BGP packets. While TTL security is most effective in protecting directly-connected BGP or LDP peers, it can also provide protection to multi-hop sessions. For multi-hop sessions the expected TTL value can be set to 255 minus the configured range of hops.

For BGP and LDP TTL security additional details, see `draft-gill-btsh-xx.txt` and `draftchen-ldp-ttl-xx.txt`.

## 2.3.7 Management Access Filter

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

### 2.3.7.1 MAF Filter Packet Match

Three different **management-access-filter** policies can be configured: **ip-filter**, **ipv6-filter**, and **mac-filter**. Each policy is an ordered list of entries. For this reason, entries must be sequenced correctly from the most to the least explicit.

Management Access filter (MAF) packet match rules:

- Each MAF policy is an ordered list of entries, therefore entries must be sequenced correctly from the most to the least explicit.
- If multiple match criteria are specified in a single MAF filter policy entry, all criteria must be met for the packet to be considered a match against that policy entry (logical AND).
- Any match criteria not explicitly defined is ignored during a match.
- A MAF filter policy entry defined without any match criteria is inactive.
- A MAF filter policy entry with match criteria defined, but no action configured, inherits the default action defined at the **management-access-filter** level.
- The **management-access-filter default-action** applies individually per IPv4, IPv6, or MAC CPM filter policies that are in a **no shutdown** state.
- When both **mac-filter** and **ip-filter** or **ipv6-filter** are to be applied to a specific packet, **mac-filter** is applied first.

### 2.3.7.2 MAF IPv4/IPv6 Filter Entry Match Criteria

Table 16 lists the supported IPv4 and IPv6 match criteria.

**Table 16** IPv4 and IPv6 Match Criteria

Criteria	Description
<b>src-ip</b>	Matches the specified source IPv4 or IPv6 address prefix and mask against the source IPv4 or IPv6 address field in the IP packet header
<b>next-header</b>	Matches the specified upper-layer protocol (such as TCP, UDP, or IGMPv6) against the next-header field of the IPv6 packet header. "*" can be used to specify a TCP or UDP upper-layer protocol match (Logical OR). Next-header matching allows also matching on presence of a subset of IPv6 extension headers. See the CLI section for details on which extension header match is supported.
<b>protocol</b>	Matches the specified protocol against the Protocol field in the IPv4 packet header (for example, TCP, UDP, or IGMP) of the outer IPv4. "*" can be used to specify TCP or UDP upper-layer protocol match (Logical OR).
<b>dst-port</b>	Matches the specified port value against the destination port number of the UDP or TCP packet header.
<b>flow-label</b>	Matches the IPv6 flow label.
router	Matches the router instance packets that are ingressing from for this filter entry.
src-port	Matches the port packets that are ingressing from for this filter entry.

### 2.3.7.3 MAF MAC Filter Entry Match Criteria

Table 17 describes the supported MAC match criteria. The criteria are evaluated against the Ethernet header of the Ethernet frame.

**Table 17** Router Instance Match Criteria

Criteria	Description
<b>frame-type</b>	Matches a specific type of frame format.
<b>src-mac</b>	Matches the specified source MAC address frames. Optionally, operators can configure a mask to be used in a match.

**Table 17 Router Instance Match Criteria (Continued)**

Criteria	Description
<b>dst-mac</b>	Matches the specified destination MAC address frames. Optionally, operators can configure a mask to be used in a match.
<b>dot1p</b>	Matches 802.1p frames. Optionally, operators can configure a mask to be used in a match.
<b>etype</b>	Matches the specified Ethernet II frames. The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame.
<b>snap-oui</b>	Matches frames with the specified three-byte OUI field.
<b>snap-pid</b>	Matches frames with the specified two-byte protocol ID that follows the three-byte OUI field.
<b>ssap</b>	Matches the specified frames with a source access point on the network node designated in the source field of the packet. Optionally, operators can configure a mask to be used in a match.
<b>dsap</b>	Matches the specified frames with a destination access point on the network node designated in the destination field of the packet. Optionally, operators can configure a mask to be used in a match.
<b>cfm-opcode</b>	Matches the specified packet with the specified <b>cfm-opcode</b> .
<b>svc-id</b>	Matches the service ID packets are ingressing from.
<b>svc-name</b>	Matches the service name packets are ingressing from.

### 2.3.7.4 MAF Filter Policy Action

A management access filters allow to **permit** or **deny** (or use deny-host-unreachable response for IP filters) traffic.

### 2.3.7.5 MAF Filter Policy Statistics and Logging

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

## 2.4 Vendor-Specific Attributes (VSAs)

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



**Note:** The PE-record entry is required to support the RADIUS Discovery for Layer 2 VPN feature. A PE-record is only relevant if the RADIUS Discovery feature is used, not for the standard RADIUS setup.

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

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

---

## 2.5 Other Security Features

This section describes the other security features supported by the SR OS.

### 2.5.1 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. This server process is separate from the SSH and SCP client commands on the routers which initiate outbound SSH and SCP sessions.

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

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

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

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

Two cipher lists, the client-cipher-list and the server-cipher-list, can be configured for negotiation of the best compatible ciphers between 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 the 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.

## 2.5.2 SSH PKI Authentication

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



**Note:** SSHv1 is not supported when the node is running in FIPS-140-2 mode.

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 typically 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.

### 2.5.2.1 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 plain text 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.

### 2.5.3 HMAC strengthening (SHA-224/256/384/512)

SR OS supports Secure Shell. Previously, the MAC algorithms were hard-coded and in a predefined order which was negotiated between server and client. There was no way to change this predefined order to tailor customer needs.

SR OS only supports SHA-1 algorithms and stronger SHA-2 algorithms are not supported.



This feature introduces two stronger HMAC SHA-2 algorithms:

- HMAC\_SHA2\_256
- HMAC\_SHA2\_512

## 2.5.4 MAC Client and Server List

In addition to stronger HMAC algorithms, this feature introduces a configurable server and client MAC list for SSHv2. This allows the user to add or remove MAC algorithms from the list. The user can program the strong HMAC algorithms on top of the configurable MAC list (for example, lowest index in the list) in the order to be negotiated first between the client and server. The first algorithm in the list that is supported by both the client and the server is the one that is agreed upon.

There are two configurable MAC lists:

- server list
- client list



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

## 2.5.5 Regenerate the ssh-key without disabling SSH

Two releases ago, SR OS did not periodically rollover the SSH symmetric key. SR OS now supports periodic rollover of the SSH symmetric key. Symmetric key rollover is important in long SSH sessions. Symmetric key rollover ensures that the encryption channel between the client and server is not jeopardized by an external hacker that is trying to break the encryption via a brute force attack.

This feature introduces symmetric key rollover on SSH client or server. The following are triggers for symmetric key rollover and negotiation:

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

For extra security, by default, the key re-exchange is enabled under SR OS. The default values are as follow:

`client`

```
        bytes 1000000000
        minutes 60
        no shutdown
    exit
server
        bytes 1000000000
        minutes 60
        no shutdown
    exit
```

### 2.5.5.1 Key re-exchange procedure

Key re-exchange is started by sending an SSH\_MSG\_KEXINIT packet while not already doing a key exchange. When this message is received, a party must respond with its own SSH\_MSG\_KEXINIT message, except in cases where the received SSH\_MSG\_KEXINIT already was a reply. Either party may initiate the re-exchange, but roles must not be changed (for example, the server remains the server, and the client remains the client).

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

RFC 4253 recommends key exchange after every hour or 1Gbytes of transmitted data, which is met by SR OS default implementation.

SR OS can roll over keys via two mechanisms:

- bytes (default is 1 Gbyte and the keys will be negotiated)
- minutes (default is 1 minute)



**Note:** If both are configured, the key rollover will happen based on whichever occurs first.



**Note:** If these parameters are changed, only new SSH connections will inherit them. The existing SSH connections will use the previously configured parameters.

## 2.5.6 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-back off 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-back off 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.

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](#). The commands are described in [Login Control Commands](#).

## 2.5.7 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).

A security or LI 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.

In addition to the security or LI event log, an SNMP trap is also generated so that any SNMP server (including the NSP NFM-P) can use the trap for an action.

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 the **show>system>security>lockout** command.

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

## 2.5.8 CLI Login Scripts

The SR OS supports automatic execution of CLI scripts when a user successfully logs into the router and starts a CLI session.

Users who authenticate via the local user database can use the configurable **configure>system>security>user user-name>console>login-exec file-url** login exec script.

A global login-script can be configured to execute a common script when any user logs into CLI. A per user login-script can also be configured to execute when a specific user logs into CLI. These login-scripts execute whether the user was authenticated via the local user database, TACACS+ or RADIUS. The scripts can be used, for example, to define a common set of CLI aliases that are made available on the router for all users.

To configure a global login exec script, use the **configure>system>login-control>login-scripts> global file-url** script.

To configure a user-specific login exec script, use the **configure>system>login-control>login-scripts>per-user>user-directory>file-url file-name file-name** script.

## 2.5.9 802.1x Network Access Control

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

## 2.5.10 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.

### 2.5.10.1 Packet Formats

```

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

```

### Option Syntax

- Kind: 8 bits

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

- Length: 8 bits

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

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

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

- T-Bit: 1 bit

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

The default value is 0.

- K-Bit: 1 bit

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

- Alg ID: 6 bits

The Alg ID field identifies the MAC algorithm.

- Res: 2 bits

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

Key ID: 6 bits

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

- Authentication Data: Variable length

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

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

## 2.5.10.2 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 18](#) shows the mapping between these attributes and the CLI command to set them.

**Table 18** Keychain Mapping

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

**Table 18 Keychain Mapping (Continued)**

Definition	CLI
Shared secret to use with key[i].	config>system>security>keychain>direction>uni>receive>entry with shared secret parameter config>system>security>keychain>direction>uni>send>entry with shared secret parameter config>system>security>keychain>direction>bi>entry with shared secret parameter
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 19](#) shows the mapping between these attributes and the CLI command to set them.

**Table 19 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



**Table 19 Security Algorithm Support Per Protocol (Continued)**

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

## 2.5.11 gRPC Authentication

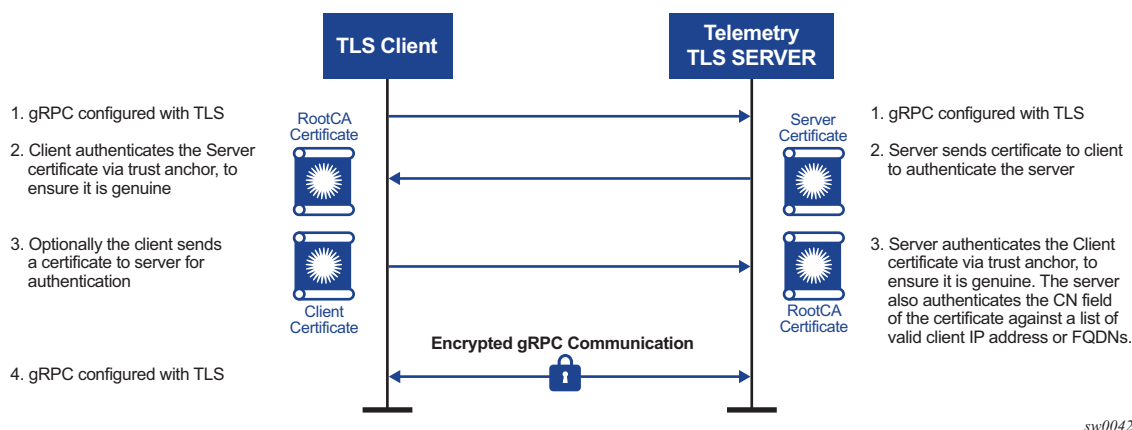
gRPC communication between the client and server must be authenticated and encrypted. There are two types of authentication:

- Authentication via session credentials — Session credentials operate similarly to device authentication, ensuring that the device is allowed in the network and is authorized by the provider. This type of authentication is performed using PKI and X.509.3 certificates. gRPC uses TLS for session authentication.  
SR OS supports TLS servers for gRPC.
- Authentication using channel credentials — Channel credentials use a user name and password that are entered at the gRPC client terminal to authenticate gRPC packets using an AAA method.

Session authentication provides proof that the client and server are authorized devices and that they belong to the provider. After authentication, the session becomes encrypted using TLS, and gRPC PDUs are transmitted between the client and server.

Figure 10 shows a basic session authentication using TLS.

**Figure 10 Session Authentication Using TLS**

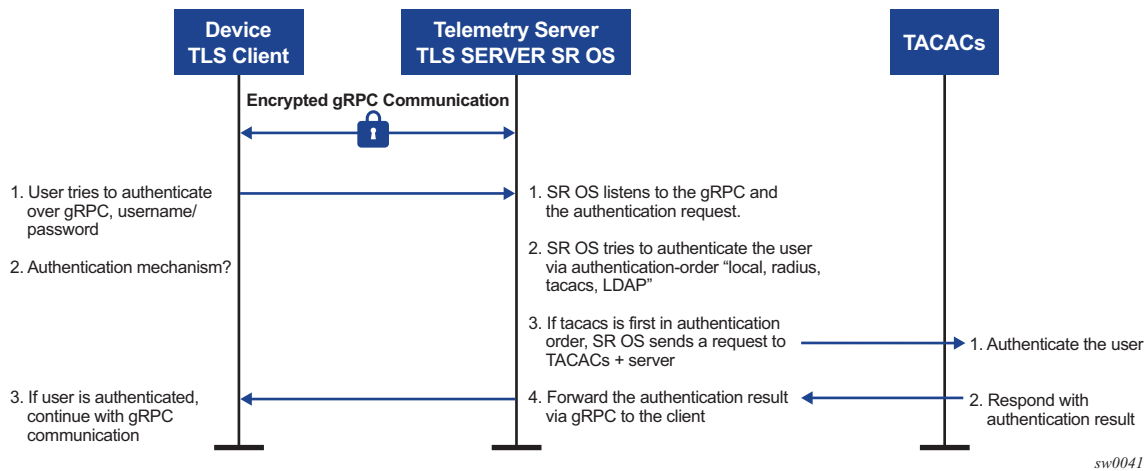


sw0042

Channel credentials use username and password authentication. Each gRPC channel packet can contain a username and a password. Authentication is done through standard SR OS authentication order and mechanisms. All current authentication methods, including local and AAA servers, are applicable to gRPC channels. In addition, all authentication orders currently used by Telnet or SSH are compatible with gNMI Call authentication.

Figure 11 shows a basic gNMI Call authentication using SR OS.

**Figure 11** gNMI Call Authentication Using SR OS



gRPC channel packets contain the username and password in clear text, and are only encrypted using TLS. If a TLS server profile is assigned to the gRPC session, all PDUs between the server and client are encrypted. If TLS becomes operationally down, no gRPC PDUs are transmitted in clear text.

SR OS relies on existing authentication mechanisms for gRPC channels, including:

- AAA servers and local authentication orders configured using the **config>system>security>password>authentication-order** command
- password complexity rules
- requiring the user to be configured as part of gRPC access by using the **config>system>security>user>access>grpc** command
- disconnecting the gRPC session by using the **admin>disconnect gNMI** command



**Note:** gRPC is not affected by password aging.

Security profiles can authorize bulk **get**, **set**, and **subscribe gRPC** commands that are received by the server. Profiles can be configured to permit or deny specific gRPC commands; for example, a profile for one user can authorize **get** and **set** commands, while a profile for another user can authorize **get** commands only.

## 2.5.12 Hash Management per Management Interface Configuration

Hash management is configurable per management interface, for example, classic CLI, MD-CLI, NETCONF, or gRPC. Each management interface will have its own write-hash algorithm. Depending on which management interface the user logs into, the write hash of that interface should be checked and used for displaying the critical phrases.

In the classic CLI interface, the read and write hash algorithms can be different, for example, hash for write and hash2 for read.

For MD-CLI, NETCONF, and gRPC interfaces, when a hash is configured, only write will be implemented using that hash algorithm. For example, if hash2 is configured, SR OS will display the phrase in hash2 format and read the phrase in all formats. The read algorithm is not affected by hash algorithm configuration and SR OS reads in all hash formats.

### 2.5.12.1 Hash encryption Using AES 256

Hash and hash2 use the AES 256 algorithm for all interfaces. However, hash2 uses module-specific text to make the hash unique per module or protocol. For example, BGP will use a different pre-pending text than IGP. This pre-pending text is appended to the key and then hashed using hash2.

Classic CLI hash has been changed to AES-256.

Upgrade from DES to AES-256 is allowed and loading a config file in classic CLI with DES to a new software that supports AES-256 is also allowed.

The DES and the DES key should only be used for decryption of the old password to obtain clear text and the password should then be rehashed using AES-256. The few characters of the old hashed phrase are used to determine that the phrase is hashed using DES.

### **2.5.12.2 Clear Text**

The cleartext option for the write algorithm displays the hash in clear text in the config file, info, info detail, and so on.

## **2.6 Configuration Notes**

This section describes security configuration restrictions.

### **2.6.1 General**

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



## 2.7 Configuring Security with CLI

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

### 2.7.1 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, TACACS+, and/or LDAP
  - One to five RADIUS, TACACS+, and/or LDAP servers
  - RADIUS, TACACS+, and/or LDAP parameters

[Table 20](#) depicts the capabilities of authentication, authorization, and accounting configurations. For example, authentication can be enabled locally and on RADIUS, TACACS+, and LDAP 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 20 Security Configuration Requirements**

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

## 2.7.2 Security Configuration Procedures

### 2.7.2.1 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 an **action** keyword specified CPM to be considered active 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.

The following CLI commands are an example of how to configure a management access filter on the 7450 ESS. This example only accepts packets matching the criteria specified in entries 1 and 2. Non-matching packets are denied.

The following is an example of a management access filter configuration that accepts packets matching the criteria specified in IP, IPv6 and MAC entries. Non-matching packets are denied for IPv4 filter and permitted for IPv6 and MAC filters.

```
*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 2001:db8:1000::/64
    next-header rsvp
```



```

        log
        action deny
    exit
exit
mac-filter
    default-action permit
    entry 12
        match frame-type ethernet_II
        svc-id 1
        src-mac 00:01:01:01:01:01 ff:ff:ff:ff:ff:ff
    exit
    action permit
    exit
exit
-----
*A:Dut-C>config>system>security>mgmt-access-filter#

```

### 2.7.2.2 Configuring IP CPM Filters

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

The configuration below is an example that follows the recommendations for SSH and BGP:

- Allow SSH from trusted subnet only
- Allow BGP from trusted subnet only
- Explicitly deny all other traffic and operationally log unexpected packets

```

A:Dut-A>config>sys>security>cpm-filter# info
-----
    default-action drop
    ip-filter
        entry 100 create
            action accept
            description "SSH: server terminated TCP sessions from truste
d subnets"

            match protocol tcp
                dst-port 22 65535
                src-ip ip-prefix-list "trusted-mgmt-subnet"
            exit
        exit
        entry 200 create
            action accept
            description "BGP: server terminated TCP Sessions"
            match protocol tcp
                dst-port 179 65535
                src-ip ip-prefix-list "trusted-bgp-subnet"
            exit
        exit
        entry 300 create
            action accept

```

```

s"
        description "BGP: client responses for initiated TCP session"
        match protocol tcp
            src-ip ip-prefix-list "trusted-bgp-subnet"
            src-port 179 65535
        exit
    exit
    entry 6000 create
        action drop
        description "Drop all other UDP"
        log 102
        match protocol udp
        exit
    exit
    entry 6010 create
        action drop
        description "drop all other TCP"
        log 103
        match protocol tcp
        exit
    exit
    no shutdown
exit
-----

```

### 2.7.2.3 Configuring IPv6 CPM Filters

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

The configuration below is an example that follows the recommendations for SSH and BGP:

- Allow SSH from trusted subnet only
- Allow BGP from trusted subnet only
- Explicitly deny all other traffic and operationally log unexpected packets

```

A:Dut-A>config>sys>security>cpm-filter# info
-----
        default-action drop
        ip-filter
            entry 100 create
                action accept
                description "SSH: server terminated TCP sessions from truste
d subnets"
                match protocol tcp
                    dst-port 22 65535
                    src-ip ip-prefix-list "trusted-mgmt-subnet"
                exit
            exit
            entry 200 create
                action accept

```

```

        description "BGP: server terminated TCP Sessions"
        match protocol tcp
            dst-port 179 65535
            src-ip ip-prefix-list "trusted-bgp-subnet"
        exit
    exit
    entry 300 create
        action accept
        description "BGP: client responses for initiated TCP session
s"

        match protocol tcp
            src-ip ip-prefix-list "trusted-bgp-subnet"
            src-port 179 65535
        exit
    exit
    entry 6000 create
        action drop
        description "Drop all other UDP"
        log 102
        match protocol udp
        exit
    exit
    entry 6010 create
        action drop
        description "drop all other TCP"
        log 103
        match protocol tcp
        exit
    exit
    no shutdown
exit
ipv6-filter
    entry 100 create
        action accept
        description "SSH: server terminated TCP sessions from truste
d subnets"

        match next-header tcp
            dst-port 22 65535
            src-ip ipv6-prefix-list "trusted-mgmt-subnet"
        exit
    exit
    entry 200 create
        action accept
        description "BGP: server terminated TCP Sessions"
        match next-header tcp
            dst-port 179 65535
            src-ip ipv6-prefix-list "trusted-bgp-subnet"
        exit
    exit
    entry 300 create
        action accept
        description "BGP: client responses for initiated TCP session
s"

        match next-header tcp
            src-ip ipv6-prefix-list "trusted-bgp-subnet"
            src-port 179 65535
        exit
    exit
    entry 6000 create

```

```

        action drop
        description "Drop all other UDP"
        log 102
        match next-header udp
        exit
    exit
    entry 6010 create
        action drop
        description "drop all other TCP"
        log 103
        match next-header tcp
        exit
    exit
    no shutdown
exit
-----

```

### 2.7.2.4 Configuring MAC CPM Filters

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#

```

### 2.7.2.5 Configuring CPM Queues

CPM queues can be used for troubleshooting purposes to provide rate limit capabilities for traffic destined to CPM as described in an earlier section of this document.

The following example displays a CPM queue configuration:

```

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

```

```

-----
        queue 101 create
            rate 100
        exit
-----
A:ALA-987>config>sys>security>cpm-queue#

```

## 2.7.2.6 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:

```

*A: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 10.1.1.13 peer 10.1.1.15 delivery-service 300
dynamic-keying
    ike-policy 1
    pre-shared-key "Sanity-1"
    transform 1
    cert
        trust-anchor "R1-0"
        cert "M2cert.der"
        key "M2key.der"
    exit
exit
no shutdown
exit
exit
exit

```

### 2.7.2.7 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 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#

```

### 2.7.2.7.1 Parameters

Matching in authorization profiles allows the use of parameters and optional parameters. A set of angle brackets <...> indicates matching on a parameter and/or optional parameter.

The following rules govern parameter matching in the CLI:

#### Rule 1

Any parameter and/or optional parameter can be present in the match string.

#### Rule 2

When a parameter and an optional parameter is present in the user-profile match string, all parameters or optional parameters to its left must also be stated/present.

#### Rule 3

The user can either specifically state or completely omit unnamed parameters in the match string, as required. However, all unnamed parameter in the CLI command must be present in the match string when matching on an unnamed parameter is used.

For example, consider the **OSPF** command:

```
*A:SwSim14# configure router ospf
- no ospf [<ospf-instance>]
- ospf [<ospf-instance>] [<router-id>]

<ospf-instance>      : [0..31]
<router-id>         : <ip-address>
```

In this case, the user can match on OSPF to allow or deny the command per user-profile, as follows:

```
Match "configure router ospf" action deny
```

Or the user can decide to only allow a certain OSPF instance for a user, as follows:

```
Match "configure router ospf <ospf-instance-value> <router-id-value>"
```



**Note:** Although the user's matching is based on <ospf-instance-value> that is "an unnamed value", all other unnamed values in the **OSPF** command (such as the <router-id-value>) must also be present in the match string.

#### Rule 4

When multiple unnamed parameters are present in the match string, the parameters must be provided in the correct order as described in the command **help** to generate the correct match behavior. For example, using the order of parameters described in the **OSPF** command usage in Rule 3 above, use the following statement for a user-profile match:

```
match "configure router ospf <ospf-instance-value> <router-id-value>
```

The desired match behavior might not be achieved if the unnamed parameters <ospf-instance-value> and <router-id-value> are out of order with respect to the help screen.

The following displays a parameter matching output:

```
config>system>security>profile# info
  entry 10
    match "show router <22> route-table "
    action permit
  exit
  entry 20
    match "configure service vprn <22>"
    action read-only
  exit
  entry 30
    match "show service id <22>"
    action permit
  exit
  entry 40
    match "configure router interface <system>"
    action deny
  exit
```

### 2.7.2.7.2 Wildcards

In addition, parameter configuration is facilitated by the availability of wildcards (.) in the OAM subtree and for commands such as **ping**, **trace-route** and **mtrace**. For example, consider the following command:

```
ping <ip-address> router 10
```

Instead of listing all the permitted IP addresses in the policy, as shown in the following example,

```
Match ping <10.0.0.1> router <10>
Action permit
Match ping <10.0.0.2> router <10>
Action permit
```



The wildcard<ip-address> parameter allows a simpler search criterion. In the following example, the use of <.\*> wildcard enables the ability to ping any address in the router 10 context, that is, any address in VRF 10:

```
Match ping <.*> router <10>
Action permit
```



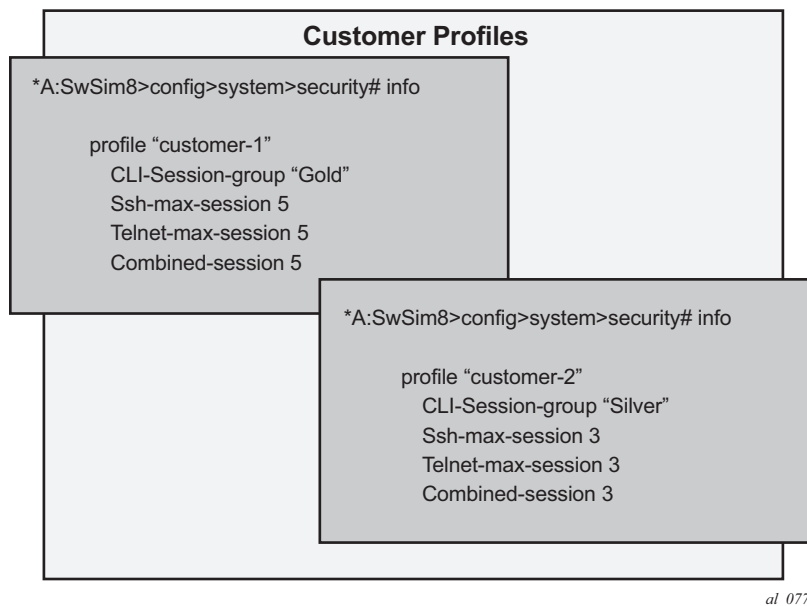
**Note:** While wildcards are available and allowed for all parameters in the OAM subtree, Nokia recommends that caution is exercised when using wildcards and limit their use to commands such as **ping**, **trace-route**, and **mtrace**. The use of wildcards in certain formats may be a security concern and result in making the IP addresses in the VRF, including the base routing table, unreachable. Or it could allow the customer to ping any IP address in the VRF, including the base routing table. This may be a potential security concern and should be avoided.

For example, the following usage is not advised:

```
Match ping <.*> router <.*>
Action permit
```

### 2.7.2.7.3 CLI Resource Management

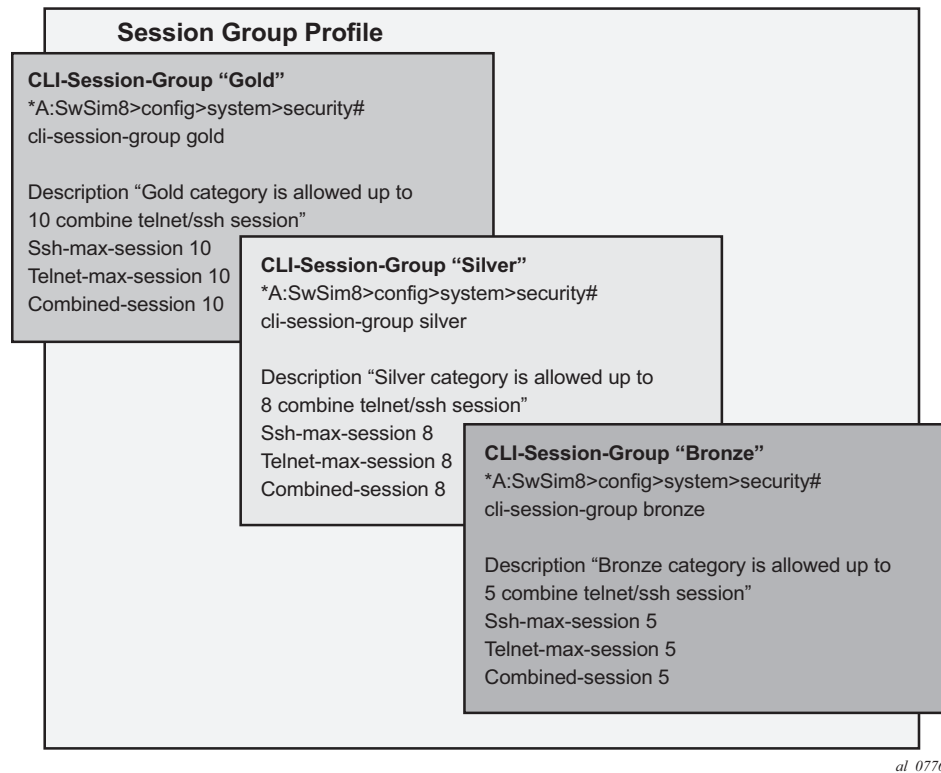
SR OS has the capability to manage telnet/ssh sessions per user and at a higher level per system. At the system level, the user can configure a **cli-session-group** for different customer priorities. The **cli-session-group** is a container that sets the maximum number of CLI sessions for a class of customers, with a unique session limit for each customer. For example, as depicted in [Figure 12](#), “Gold” category customers can have a **cli-session-group** that allows them more telnet/ssh sessions compared to “Silver” category customers.

**Figure 12 cli-session-group for Customer Classes**

The configured **cli-session-group** can be assigned to user-profiles. At the user profile level, each profile can be configured with its own max ssh/telnet session and it will be policed/restricted by the higher order **cli-session-group** that is assigned to it.

As depicted in [Figure 13](#), the final picture is a hierarchical configuration with top-level cli-session-groups that control each customer's total number of SSH or telnet sessions and the user-profile for each user for that customer.

**Figure 13 Hierarchy of cli-session-group Profiles**



Every profile will subtract one from it's corresponding **max-session** when a TELNET or SSH session is established in the following cases:

- where multiple profiles are configured under a user
- where multiple profiles arrive from different AAA servers (Local Profile, RADIUS Profile or TACACS Profile)

The first profile to run out of corresponding **max-session** will limit future TELNET or SSH sessions. In other words, while each profile for the user can have its independent **max-session**, only the lowest one will be honored. If the profile with the lowest **max-session** is removed, the next lower profile **max-session** will be honored and so on. All profiles for a user are updated when a TELNET or SSH session is established.

For information about login control, see [Configuring Login Controls](#).

Use the following CLI commands to configure CLI session resources:

**CLI Syntax:**     `config>system>security>profile <name>`  
                               `[no] ssh-max-sessions session-limit`

```
[no] telnet-max-sessions session-limit
[no] combined-max-session session-limit
[no] cli-session-group session-group-name
```

### 2.7.2.8 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#
```

### 2.7.2.9 Configuring Keychains

The following displays a keychain configuration.

```
A:ALA-1>config>system>security# info
-----
...
        keychain "abc"
            direction
                bi
                    entry 1 key "ZcvSElJzJx/wBZ9biCtOVQJ9YZQvVU.S" hash2 alg
orithm aes-128-cmac-96
                    begin-time 2006/12/18 22:55:20
                exit
            exit
        exit
    exit
    keychain "basasd"
        direction
            uni
                receive
                    entry 1 key "Ee7xdKlYO2D0m7v3IJv/84LIu96R2fZh" hash2
```

```

algorithm aes-128-cmac-96
                                tolerance forever
                                exit
                                exit
                                exit
                                exit
                                exit
                                exit
...
-----
A:ALA-1>config>system>security#

```

## 2.7.2.10 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.

### 2.7.2.10.1 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:** 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#

```

### 2.7.2.10.2 Profile

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

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

The following output displays the copied profiles:

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

```
        no description
        match "exit"
        action permit
    exit
    entry 30
        no description
        match "help"
        action permit
    exit
    entry 40
        no description
        match "logout"
        action permit
    exit
    entry 50
        no description
        match "password"
        action permit
    exit
    entry 60
        no description
        match "show config"
        action deny
    exit
    entry 70
        no description
        match "show"
        action permit
    exit
    entry 80
        no description
        match "enable-admin"
        action permit
    exit
    exit
    profile "administrative"
        default-action permit-all exit
    ...
-----
A:ALA-12>config>system>security#
```

## 2.7.3 RADIUS Configurations

### 2.7.3.1 Configuring RADIUS Authentication

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



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, 7750 SR, 7950 XRS, and VSR 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#
```

### 2.7.3.2 Configuring RADIUS Authorization

In order for RADIUS authorization to function, RADIUS authentication *must* be enabled first. See [Configuring RADIUS Authentication](#).

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

On the local router, use the following 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#
```

### 2.7.3.3 Configuring RADIUS Accounting

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

**CLI Syntax:**

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

The following 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#
```

## 2.7.4 Configuring 802.1x RADIUS Policies

Use the following CLI commands to configure generic authentication parameters for clients using 802.1x EAPOL. Additional parameters are configured per Ethernet port. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*.

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

**CLI Syntax:**

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

The following displays a 802.1x configuration example:

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

## 2.7.5 TACACS+ Configurations

### 2.7.5.1 Enabling TACACS+ Authentication

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

Use the following CLI commands to configure 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#
```

## 2.7.5.2 Configuring TACACS+ Authorization

In order for TACACS+ authorization to function, TACACS+ authentication *must* be enabled first. See [Enabling TACACS+ Authentication](#).

On the local router, use the following CLI commands to configure 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#
```

### 2.7.5.3 Configuring TACACS+ Accounting

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

**CLI Syntax:**   config>system>security  
                  tacplus  
                  accounting

The following 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#
```

### 2.7.5.4 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#
```

## 2.7.6 LDAP Configurations

### 2.7.6.1 Configuring LDAP Authentication

LDAP is disabled by default and must be explicitly enabled. To use LDAP authentication on the router, configure one or more LDAP servers on the network.

TLS certificates and clients must also be configured. Refer to the “TLS” section of the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* for more information about configuring TLS.

Use the following CLI commands to configure LDAP:

```
CLI Syntax:  config>system>security>ldap
                [no] public-key-authentication
                [no] retry
                [no] server
                [no] shutdown
                [no] timeout
                [no] use-default-template

                config>system>security>password
                  authentication-order [method] exit-on-reject

                config>system>security>ldap
                  public-key-authentication
                  server server-index create
                    address ip-address port port
                    bind-authentication root-dn [password
                      password] [hash | hash2]
                    ldap-server server-name
                    search base-dn
                    tls-profile tls-profile-name
                    no shutdown
                  exit
                  no shutdown
```

The following displays an LDAP authentication configuration example:

```
A:SwSim14>config>system>security>ldap#
-----
[no] public-key-authentication
[no] retry
[no] server
[no] shutdown
[no] timeout
[no] use-default-template
```

```

-----
*A:SwSim14>config>system>security>password#
-----
    authentication-order [local | radius | tacplus | ldap] exit-on-reject
-----
*A:SwSim14>config>system>security>ldap# info
-----
    public-key-authentication
    server 1 create
        address 10.1.1.1
        bind-authentication "cn=administrator,cn=users,dc=nacblr2,dc=example,dc=com
        password"
        ldap-server "active-server"
        search "dc=sns,dc=example,dc=com"
        tls-profile "server-1-profile"
        no shutdown
    exit
    no shutdown
-----
*A:SwSim8>config>system>security>tls# info
-----
    client-tls-profile "server-1-profile" create
        cipher-list "to-active-server"
        trust-anchor-profile "server-1-ca"
    no shutdown
    exit

```

## 2.7.6.2 Configuring Redundant Servers

Up to five redundant LDAP servers can be configured. The following examples show configuration of two servers, Server-1 and Server-5.

### Configuration of Server-1:

```

A*:SwSim14>config>system>security>ldap# info
    public-key-authentication
    server 1 create
        address 10.1.1.1
        ldap-server "active-server"
        tls-profile "server-1-profile"

A*:SwSim14>config>system>security>tls# info
    client-tls-profile "server-1-profile" create
        cert-profile "client-cert-profile"
        cipher-list "to-active-server"
        trust-anchor-profile "server-1-ca"
    no shutdown
    exit

```

### Configuration of Server-5 (backup):

```

A*:SwSim14>config>system>security>ldap# info
    public-key-authentication
    server 5 create

```

```
address 10.5.5.1
ldap-server "backup-server-5"
tls-profile "server-5-profile"

A*:SwSim14>config>system>security>tls# info
client-tls-profile "server-5-profile" create
cert-profile "client-cert-profile"
cipher-list "to-backup-server-5"
trust-anchor-profile "server-5-ca"
no shutdown
exit
```

### 2.7.6.3 Enabling SSH

SSH must be enabled to use LDAP authentication. See [Enabling SSH](#) for more information.

## 2.7.7 Configuring Login Controls

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

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



## 2.8 Security Configuration Command Reference

### 2.8.1 Command Hierarchies

- Security Commands
  - LLDP Commands
  - Management Access Filter Commands
  - CLI Script Authorization Commands
  - CPM Filter Commands
  - CPM Queue Commands
  - CPU Protection Commands
  - Distributed CPU Protection Commands
  - Extracted Protocol Traffic Priority Commands
  - Security Password Commands
  - Public Key Infrastructure (PKI) Commands
  - Profile Commands
  - CLI Session Commands
  - RADIUS Commands
  - TACACS+ Client Commands
  - LDAP Commands
  - User Management Commands
  - User Template Commands
  - Dot1x Commands
  - Keychain Commands
  - TTL Security Commands
  - gRPC Commands
- Login Control Commands

#### 2.8.1.1 Security Commands

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

- 
- [no] **ftp-server**
  - **management-interface**
    - **classic-cli**
      - **read-algorithm** {hash | hash2 | all-hash}
      - **no read-algorithm**
      - **write-algorithm** {hash | hash2 | cleartext}
      - **no write-algorithm**
    - **grpc**
      - **hash-algorithm** {hash | hash2 | cleartext}
      - **no hash-algorithm**
    - **md-cli**
      - **hash-algorithm** {hash | hash2 | cleartext}
      - **no hash-algorithm**
    - **netconf**
      - **hash-algorithm** {hash | hash2 | cleartext}
      - **no hash-algorithm**
  - **management**
    - [no] **allow-ftp**
    - [no] **allow-ssh**
    - [no] **allow-telnet**
    - [no] **allow-telnet6**
  - [no] **per-peer-queuing**
  - **source-address**
    - **application** app [ip-int-name | ip-address]
    - **no application** app
    - **application6** app ipv6-address
    - **no application6**
  - **ssh**
    - **client-cipher-list protocol-version version**
      - **cipher** index name cipher-name
      - **no cipher** index
    - **client-mac-list**
      - **mac** index name mac-name
      - **no mac** index
    - **key-re-exchange**
      - **client**
        - **mbytes** {mbytes | disable}
        - **no mbytes**
        - **minutes** {minutes | disable}
        - **no minutes**
        - [no] **shutdown**
      - **server**
        - **mbytes** {mbytes | disable}
        - **no mbytes**
        - **minutes** {minutes | disable}
        - **no minutes**
        - [no] **shutdown**
    - [no] **preserve-key**
    - **server-cipher-list protocol-version version**
      - **cipher** index name cipher-name
      - **no cipher** index
    - **server-mac-list**
      - **mac** index name mac-name
      - **no mac** index

- [no] **server-shutdown**
- [no] **version** *ssh-version*
- [no] **telnet-server**
- [no] **telnet6-server**
- **vprn-network-exceptions** *number seconds*
- no **vprn-network-exceptions**

### 2.8.1.1.1 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
```

### 2.8.1.1.2 Management Access Filter Commands

- ```
config
  — system
    — security
      — [no] management-access-filter
        — [no] ip-filter
          — default-action {permit | deny | deny-host-unreachable}
          — [no] entry entry-id
            — action {permit | deny | deny-host-unreachable}
            — no action
            — description description-string
            — no description
            — dst-port value [mask]
            — no dst-port
            — [no] log
            — protocol protocol-id
            — no protocol
            — router service name service-name
            — router router-instance
            — no router
            — src-ip {ip-prefix/mask | ip-prefix netmask}
```

---

```

    — no src-ip
    — src-port {port-id | cpm | lag lag-id}
    — no src-port
    — renum old-entry-number new-entry-number
    — [no] shutdown
— [no] ipv6-filter
    — default-action {permit | deny | deny-host-unreachable}
    — [no] entry entry-id
        — action {permit | deny | deny-host-unreachable}
        — no action
        — description description-string
        — no description
        — dst-port value [mask]
        — no dst-port
        — flow-label value
        — no flow-label
        — [no] log
        — next-header next-header
        — no next-header
        — router service name {service-name}
        — router {router-instance}
        — no router
        — src-ip {ipv6-address | prefix-length}
        — no src-ip
        — src-port {port-id | cpm | lag lag-id}
        — no src-port
    — renum old-entry-number new-entry-number
    — [no] shutdown
— [no] mac-filter
    — default-action {permit | deny}
    — [no] entry entry-id
        — action {permit | deny}
        — 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}
            — no snap-oui
            — 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**

### 2.8.1.1.3 CLI Script Authorization Commands

- ```

config
  — system
    — security
      — cli-script
        — authorization
          — cron
            — cli-user user-name
            — no cli-user
          — event-handler
            — cli-user user-name
            — no cli-user
          — vsd
            — cli-user user-name
            — no cli-user

```

### 2.8.1.1.4 CPM Filter Commands

- ```

config
  — system
    — security
      — [no] cpm-filter
        — default-action {accept | drop}
        — [no] ip-filter
          — [no] entry entry-id
            — action [accept | drop | queue queue-id ]
            — no action
            — description description-string
            — no description
            — log log-id
            — no log
            — match [protocol protocol-id]
            — no match
              — dscp dscp-name
              — no dscp
              — dst-ip {ip-address/mask | ip-address netmask | ip-prefix-list prefix-list-name}
              — no dst-ip
              — 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
— 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 tcp/udp port-number [mask]
— port port-list port-list-name
— port range tcp/udp port-number tcp/udp port-
   number
— no port
— router {router-instance}
— router service-name {service-name}
— src-ip [ip-address/mask | ip-address netmask |
   ip-prefix-list prefix-list-name]
— no src-ip
— src-port [src-port-number] [mask]
— src-port tcp/udp port-number [mask]
— src-port port-list port-list-name
— src-port range tcp/udp port-number tcp/udp port-
   number
— 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
— [no] ipv6-filter
   — [no] entry entry-id
      — action [accept | drop | queue queue-id ]
      — no action
      — description description-string
      — no description
      — log log-id
      — no log
      — match [next-header next-header]
      — no match
         — dscp dscp-name
         — no dscp
         — dst-ip ipv6-address/prefix-length
         — dst-ip ipv6-prefix-list ipv6-prefix-list-name
         — no dst-ip
         — 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**
  - **flow-label** *value*
  - **no flow-label**
  - **fragment** {true | false}
  - **no fragment**
  - **hop-by-hop-opt** {true | false}
  - **no hop-by-hop-opt**
  - **icmp-code** *icmp-code*
  - **no icmp-code**
  - **icmp-type** *icmp-type*
  - **no icmp-type**
  - **port** *tcp/udp port-number* [*mask*]
  - **port** **port-list** *port-list-name*
  - **port** **range** *start end*
  - **no port**
  - **router service-name** *service-name*
  - **router** *router-instance*
  - **no router**
  - **src-ip** [*ipv6-address/prefix-length*] [**ipv6-prefix-list** *ipv6-prefix-list-name*]
  - **no src-ip**
  - **src-port** [*src-port-number*] [*mask*]
  - **no src-port**
  - **tcp-ack** {true | false}
  - **no tcp-ack**
  - **tcp-syn** {true | false}
  - **no tcp-syn**
  - **renum** *old-entry-id new-entry-id*
  - [no] **shutdown**
  - [no] **mac-filter**
    - [no] **entry** *entry-id*
      - **action** [accept | drop | queue *queue-id*]
      - **no action**
      - **description** *description-string*
      - **no description**
      - **log** *log-id*
      - **no log**
      - **match** [**frame-type** *frame-type*]
      - **no match**
        - **cfm-opcode** {lt | gt | eq} *opcode*
        - **cfm-opcode** **range** *start end*
        - **no cfm-opcode**
        - **dsap** *dsap-value* [*dsap-mask*]
        - **dst-mac** *ieee-address* [*ieee-address-mask*]
        - **no dst-mac**
        - **etype** *0x0600..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**

### 2.8.1.1.5 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

```

### 2.8.1.1.6 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

```



- **protocol-protection** [allow-sham-links][block-pim-tunneled]
- **no protocol-protection**

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide: VLL, VPLS, PBB, and EVPN*, the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* and the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter 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 for command syntax and usage for applying CPU protection policies. Examples of entities that can have CPU protection policies applied to them include:

```
config>router>if>cpu-protection policy-id
```

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

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

```
config>service>ies>if>cpu-protection policy-id
```

```
config>service>ies>if>sap>cpu-protection policy-id [mac-monitoring] | [eth-  
cfm-monitoring [aggregate] [car]]
```

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

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

```
config>service>vpls>video-interface>cpu-protection policy-id
```

```
config>service>vprn>if>cpu-protection policy-id
```

```
config>service>vprn >if>sap>cpu-protection policy-id [mac-monitoring] | [eth-  
cfm-monitoring [aggregate] [car]]
```

```
config>service>vprn>nw-if>cpu-protection policy-id
```

```
config>service>vprn>sub-if>grp-if>sap>cpu-protection policy-id [mac-  
monitoring] | [eth-cfm-monitoring [aggregate] [car]]
```

```
config>subscr-mgmt>msap-policy>cpu-protection policy-id [mac-monitoring]
```

### 2.8.1.1.7 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
            — exceed-action {discard | low-priority | 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
          — protocol name [create]
          — no protocol name
            — dynamic-parameters
              — 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
            — 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
    — fp
      — dist-cpu-protection

```

- [no] **dynamic-enforcement-policer-pool** *number-of-policers*

### 2.8.1.1.8 Extracted Protocol Traffic Priority Commands

```

config
  — card
    — fp
      — init-extract-prio-mode {uniform | l3-classify}

```

### 2.8.1.1.9 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] [method-4]
          [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 size
        — no history-size
        — minimum-age [days days] [hrs hours] [min minutes] [sec seconds]
        — no minimum-age

```

- **minimum-change** *distance*
- **no minimum-change**

### 2.8.1.1.10 Public Key Infrastructure (PKI) Commands

The following commands apply only to the 7450 ESS and 7750 SR:

```

config
  — system
    — security
      — pki
        — ca-profile name [create]
        — no ca-profile name
          — cert-file filename
          — no cert-file
          — cmpv2
            — [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]
            — url url-string [service-name service-name]
            — no url
          — crl-file filename
          — no crl-file
          — ocsp
            — responder-url url-string
            — no responder-url
            — service service-id
            — service name service-name
            — no service
        — certificate-display-format {ascii | utf8}
        — certificate-expiration-warning hours [repeat repeat-hours]
        — no certificate-expiration-warning
        — common-name-list name [create]
          — [no] cn index type type value common-name-value
        — crl-expiration-warning hours [repeat repeat-hours]
        — no crl-expiration-warning
        — maximum-cert-chain-depth level
        — no maximum-cert-chain-depth

```



**Note:** For information about CMPv6 admin certificate commands listed in the following tree, see the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter Guide*.

```
admin
  — certificate
    — clear-ocsp-cache [entry-id]
    — crl-update ca ca-profile-name
    — 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 curve {secp256r1 | secp384r1 | secp521r1}
    — gen-keypair url-string [size {512 | 1024 | 2048}] [type {rsa | dsa}]
    — gen-local-cert-req keypair url-string subject-dn subject-dn [domain-name name] [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]
    — secure-nd-export
    — secure-nd-import input url-string format input-format [password password] [key-rollover]
```

### 2.8.1.1.11 Profile Commands

```
config
  — system
    — security
      — [no] profile user-profile-name
        — combined-max-sessions session-limit
        — no combined-max-sessions
        — default-action {deny-all | permit-all | none | read-only-all}
        — [no] entry entry-id
          — action {deny | permit | read-only}
          — description description-string
          — no description
          — match command-string
          — no match
        — grpc
          — rpc-authorization
            — gnmi-capabilities {deny | permit}
            — gnmi-get {deny | permit}
            — gnmi-set {deny | permit}
            — gnmi-subscribe {deny | permit}
            — rib-api-getversion {deny | permit}
            — rib-api-modify {deny | permit}
        — [no] li
        — renum old-entry-number new-entry-number
        — ssh-max-sessions session-limit
        — no ssh-max-sessions
```

- **telnet-max-sessions** *session-limit*
- **no telnet-max-sessions**

### 2.8.1.1.12 CLI Session Commands

- ```

config
  — system
    — security
      — cli-session-group session-group-name [create]
        — combined-max-sessions number-of-sessions
        — no combined-max-sessions
        — ssh-max-sessions number-of-sessions
        — no ssh-max-sessions
        — telnet-max-sessions number-of-sessions
        — no telnet-max-sessions

```

### 2.8.1.1.13 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

```

### 2.8.1.1.14 TACACS+ Client 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**

### 2.8.1.1.15 LDAP Commands

- ```

config
  — system
    — security
      — [no] ldap
        — [no] public-key-authentication
        — retry count
        — no retry
        — server server-index [create]
        — no server server index
          — address ip-address [port port]
          — no address
          — bind-authentication root-dn [password password] [hash | hash2]
          — no bind-authentication
          — ldap-server server-name
          — no ldap-server
          — search base-dn
          — no search
          — [no] shutdown
          — tls-profile tls-profile-name
          — no tls-profile
        — [no] shutdown
        — timeout seconds
        — no timeout
        — [no] use-default-template

```

### 2.8.1.1.16 User Management Commands

- ```

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

```

- [no] **access** [ftp] [snmp] [console] [li] [netconf] [grpc]
- **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*]
- **public-keys**
  - **ecdsa**
    - [no] **ecdsa-key** *key-id* [create]
      - **description** *description-string*
      - **no description**
      - **key-value** *public-key-value*
      - **no key-value**
  - **rsa**
    - [no] **rsa-key** *key-id* [create]
      - **description** *description-string*
      - **no description**
      - **key-value** *public-key-value*
      - **no key-value**
- [no] **restricted-to-home**
- **snmp**
  - **authentication** {[none] | [[hash] {md5 *key-1* | sha *key-1*}  
privacy {none | des-key *key-2* | aes-128-cfb-key *key-2*}]}
  - **no authentication**
  - **group** *group-name*
  - **no group**

### 2.8.1.1.17 User Template Commands

- config
  - system
    - **security**
      - **user-template** {tacplus\_default | radius\_default | ldap-default}
        - [no] **access** [ftp] [console] [grpc]
        - **console**
          - **login-exec** *url-prefix::source-url*
          - **no login-exec**
        - **home-directory** *url-prefix* [*directory*] [*directory/directory..*]
        - **no home-directory**
        - **profile** *user-profile-name*
        - **no profile**
        - [no] **restricted-to-home**



### 2.8.1.1.18 Dot1x Commands

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

### 2.8.1.1.19 Keychain Commands

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

- [no] **shutdown**
- **tolerance** [*seconds* | **forever**]
- **no tolerance**
- **send**
  - **entry** *entry-id* **key** [*authentication-key* | *hash-key* | *hash2-key*] [**hash** | **hash2**] **algorithm**
  - **no entry** *entry-id*
    - **begin-time** *date* *hours-minutes* [UTC]
    - **begin-time** {**now** | **forever**}
    - **no begin-time**
    - [no] **shutdown**
- [no] **shutdown**
- **tcp-option-number**
  - **receive** *option-number*
  - **no receive**
  - **send** *option-number*
  - **no send**

#### 2.8.1.1.20 TTL Security Commands

- ```

config
  — router
    — bgp
      — group
        — ttl-security min-ttl-value
        — neighbor
          — ttl-security min-ttl-value

config
  — router
    — ldp
      — tcp-session-parameters
        — peer-transport
          — ttl-security min-ttl-value

config
  — system
    — login-control
      — ssh
        — ttl-security

config
  — system
    — login-control
      — telnet
        — ttl-security

```

### 2.8.1.1.21 gRPC Commands

```
config
  — system
    — grpc
      — [no] allow-unsecure-connection
      — gnmi
        — [no] auto-config-save
        — [no] shutdown
      — max-msg-size number
      — no max-msg-size
      — rib-api
        — purge-timeout seconds
        — no purge-timeout
        — [no] shutdown
      — [no] shutdown
      — tcp-keepalive
        — idle-time idle
        — no idle-time
        — interval interval
        — no interval
        — retries count
        — no retries
        — [no] shutdown
      — tls-server-profile name
      — no tls-server-profile
```

### 2.8.1.2 Login Control Commands

```
config
  — system
    — login-control
      — [no] exponential-backoff
      — ftp
        — inbound-max-sessions number-of-sessions
        — no inbound-max-sessions
      — idle-timeout {minutes | disable}
      — no idle-timeout
      — [no] login-banner
      — login-scripts
        — global file-url
        — no global
        — per-user user-directory file-url file-name file-name
        — no per-user
      — 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 number-of-sessions
```

- **no inbound-max-sessions**
- **outbound-max-sessions** *number-of-sessions*
- **no outbound-max-sessions**
- **ttl-security** *min-ttl-value*
- **telnet**
  - **enable-graceful-shutdown**
  - **inbound-max-sessions** *number-of-sessions*
  - **no inbound-max-sessions**
  - **outbound-max-sessions** *number-of-sessions*
  - **no outbound-max-sessions**
  - **ttl-security** *min-ttl-value*

## 2.8.2 Command Descriptions

This section provides the CLI command descriptions. Topics include:

- [Security Commands](#)
- [Security Commands](#)
- [LLDP Commands](#)
- [Login Control Commands](#)
- [Management Access Filter Commands](#)
- [Security Password Commands](#)
- [Public Key Infrastructure \(PKI\) Commands](#)
- [Profile Commands](#)
- [User Management Commands](#)
- [CLI Session Commands](#)
- [RADIUS Commands](#)
- [TACACS+ Client Commands](#)
- [LDAP Client Commands](#)
- [Dot1x Commands](#)
- [Keychain Authentication](#)
- [CLI Script Authorization Commands](#)
- [CPM Filter Commands](#)
- [CPM Queue Commands](#)
- [TTL Security Commands](#)
- [CPU Protection Commands](#)
- [Distributed CPU Protection Commands](#)
- [Extracted Protocol Traffic Priority Commands](#)

## 2.8.2.1 General Security Commands

### description

<b>Syntax</b>	<b>description</b> <i>description-string</i> <b>no description</b>
<b>Context</b>	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry config>sys>sec>cpm>ip-filter>entry config>sys>sec>cpm>ipv6-filter>entry config>sys>sec>cpm>mac-filter>entry config>system>security>dist-cpu-protection>policy config>system>security>keychain config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry config>system>security>keychain>direction>uni>send>entry config>system>security>pki>ca-profile config>sys>security>cpu-protection>policy config>system>security>mgmt-access-filter>mac-filter>entry config>system>security>cpm-filter>mac-filter>entry config>system>security>user>public-keys>ecdsa>ecdsa-key config>system>security>user>public-keys>rsa>rsa-key
<b>Description</b>	<p>This command creates a text description stored in the configuration file for a configuration context.</p> <p>This 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.</p>
<b>Default</b>	No description associated with the configuration context.
<b>Parameters</b>	<i>description-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, and so on), 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 config>system>security>mgmt-access-filter>ipv6-filter config>sys>sec>cpm>ip-filter config>system>security>keychain config>system>security>keychain>direction>bi>entry

```
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry
config>system>security>dot1x
config>system>security>dot1x>radius-plcy
config>system>security>pki>ca-profile
config>sys>sec>cpm>ipv6-filter
config>sys>sec>cpm>mac-filter>entry
```

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

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

**Default** no shutdown

### 2.8.2.2 Security Commands

#### security

**Syntax** **security**

**Context** config>system

**Description** This command enables the context to configure security settings.

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

#### copy

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

**Context** config>system>security

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

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

*dest-profile* — Specifies 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.

---

## ftp-server

<b>Syntax</b>	<b>[no] ftp-server</b>
<b>Context</b>	config>system>security
<b>Description</b>	<p>This command enables FTP servers running on the system.</p> <p>FTP servers are disabled by default. At system startup, only SSH servers are enabled.</p> <p>The <b>no</b> form of the command disables FTP servers running on the system.</p>

## management-interface

<b>Syntax</b>	<b>management-interface</b>
<b>Context</b>	config>system>security
<b>Description</b>	<p>This command enables the context for choosing a management interface for hash configuration. The management interfaces are <b>classic-cli</b>, <b>md-cli</b>, <b>netconf</b>, or <b>grpc</b>.</p>

## classic-cli

<b>Syntax</b>	<b>classic-cli</b>
<b>Context</b>	config>system>security>management-interface
<b>Description</b>	<p>This command enables the context to configure hash-control for the classic CLI interface.</p>

## read-algorithm

<b>Syntax</b>	<b>read-algorithm {hash   hash2   all-hash}</b> <b>no read-algorithm</b>
<b>Context</b>	config>system>security>management-interface>classic-cli
<b>Description</b>	<p>This command assigns a global read algorithm for the system. The read algorithm is used to read the input phrase in a module.</p> <p>The <b>no</b> form of this command reverts to the default value.</p>
<b>Default</b>	read-algorithm all-hash
<b>Parameters</b>	<p><b>hash</b> — Specifies hash. Use this option to transport a phrase between modules and nodes. In this case the write-algorithm should be <b>hash</b> as well.</p> <p><b>hash2</b> — Specifies hash2 which is module-specific.</p>

---

**all-hash** — Specifies that the system accepts hash or hash2.

## write-algorithm

<b>Syntax</b>	<b>write-algorithm {hash   hash2   cleartext}</b> <b>no write-algorithm</b>
<b>Context</b>	config>system>security>management-interface>classic-cli
<b>Description</b>	<p>This command assigns a global write algorithm for the system. The write algorithm is used to display the phrase in the config file, info, show commands, and so on.</p> <p>The <b>no</b> form of this command reverts to the default value.</p>
<b>Default</b>	write-algorithm hash2
<b>Parameters</b>	<p><b>hash</b> — Specifies hash. Use this option to transport a phrase between modules and nodes. In this case the read-algorithm should be <b>hash</b> as well.</p> <p><b>hash2</b> — Specifies hash2 which is module-specific.</p> <p><b>cleartext</b> — Specifies that the phrase is displayed as clear text everywhere.</p>

## grpc

<b>Syntax</b>	<b>grpc</b>
<b>Context</b>	config>system>security>management-interface
<b>Description</b>	This command enters the context to configure hash-control for the gRPC interface.

## hash-algorithm

<b>Syntax</b>	<b>hash-algorithm {hash   hash2   cleartext}</b> <b>no hash-algorithm</b>
<b>Context</b>	config>system>security>management-interface>grpc config>system>security>management-interface>md-cli config>system>security>management-interface>netconf
<b>Description</b>	<p>This command assigns a global read and write algorithm for the system. When the hash algorithm is set, the system will read and write the phrase based on the chosen algorithm.</p> <p>The <b>no</b> form of this command reverts to the default value.</p>
<b>Default</b>	hash-algorithm hash2



---

<b>Parameters</b>	<b>hash</b> — Specifies hash. Use this option to transport a phrase between modules and nodes. <b>hash2</b> — Specifies hash2 which is module-specific. <b>cleartext</b> — Specifies that the phrase is displayed as clear text everywhere.
-------------------	---

## md-cli

<b>Syntax</b>	<b>md-cli</b>
<b>Context</b>	config>system>security>management-interface
<b>Description</b>	This command enables the context to configure hash-control for the MD-CLI interface.

## netconf

<b>Syntax</b>	<b>netconf</b>
<b>Context</b>	config>system>security>management-interface
<b>Description</b>	This command enables the context to configure hash-control for the Netconf interface.

## management

<b>Syntax</b>	<b>management</b>
<b>Context</b>	config>system>security
<b>Description</b>	This command enables the context to allow access to management servers.

## allow-ftp

<b>Syntax</b>	<b>[no] allow-ftp</b>
<b>Context</b>	config>system>security>management
<b>Description</b>	This command allows access to the FTP server from Base and Management routers if it is operationally up.  The <b>no</b> form of this command disallows access to the FTP server.
<b>Default</b>	allow-ftp

## allow-ssh

<b>Syntax</b>	<b>[no] allow-ssh</b>
<b>Context</b>	config>system>security>management
<b>Description</b>	<p>This command allows the SSH parameters to be configured from Base and Management routers.</p> <p>The <b>no</b> form of this command disallows SSH parameters from being configured.</p>
<b>Default</b>	allow-ssh

## allow-telnet

<b>Syntax</b>	<b>[no] allow-telnet</b>
<b>Context</b>	config>system>security>management
<b>Description</b>	<p>This command allows access to the Telnet server from Base and Management routers if it is operationally up.</p> <p>The <b>no</b> form of this command disallows access to the Telnet server.</p>
<b>Default</b>	allow-telnet

## allow-telnet6

<b>Syntax</b>	<b>[no] allow-telnet</b>
<b>Context</b>	config>system>security>management
<b>Description</b>	<p>This command allows access to the Telnet IPv6 server from Base and Management routers if it is operationally up.</p> <p>The <b>no</b> form of this command disallows access to the Telnet IPv6 server.</p>
<b>Default</b>	allow-telnet6

## per-peer-queuing

<b>Syntax</b>	<b>[no] per-peer-queuing</b>
<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>

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

**Default** per-peer-queuing

## source-address

**Syntax** **source-address**

**Context** config>system>security

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

This feature only applies to inband interfaces and does not apply to the out of band management interface. Packets going out the management interface will keep using that as source IP address. In other words, when the RADIUS server is reachable through both the management interface and a network interface, the management interface is used despite whatever is configured by the source-address command.

When a source address is specified for the **ptp** 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.

## application

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

**Context** config>system>security>source-address

**Description** This command configures the source IP address specified by the **source-address** command.

The **no** form of the command removes the interface name or address from the command.

**Parameters** *app* — Specifies the application name.

**Values** cflowd, dns, ftp, ntp, ldap, ping, ptp, radius, sflow, snmptrap, snmp, ssh, syslog, tacplus, telnet, traceroute, mcreporter, icmp-error

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

---

## application6

<b>Syntax</b>	<b>application6</b> <i>app ipv6-address</i> <b>no application6</b>
<b>Context</b>	config>system>security>source-address
<b>Description</b>	<p>This command specifies the application to use the source IPv6 address specified by the <b>source-address</b> command.</p> <p>The <b>no</b> form of the command removes the application and IPv6 address from the configuration.</p>
<b>Parameters</b>	<p><i>app</i> — Specifies the application name.</p> <p><b>Values</b>      cflowd, dns, ftp, ldap, ntp, ping, radius, sflow, snmptrap, sntp, ssh, syslog, tacplus, telnet, traceroute, icmp6-error</p> <p><i>ipv6-address</i> — Specifies the IPv6 address.</p>

## ssh

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

## client-cipher-list

<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 the configuration of a 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 2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2</p>

## cipher

<b>Syntax</b>	<b>cipher</b> <i>index name cipher-name</i> <b>no cipher</b> <i>index</i>
---------------	--

- Context** config>system>security>ssh>client-cipher-list  
config>system>security>ssh>server-cipher-list
- Description** This command enables the 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.
- The **no** form of the command removes the index and cipher name from the configuration.
- Default** no cipher *index*
- Parameters** *index* — Specifies the index of the cipher in the list.
- Values** 1 to 255
- cipher-name* — Specifies the algorithm used when performing encryption or decryption.
- Values** For SSHv1:  
Client ciphers: des, 3des, blowfish  
Server ciphers: 3des, blowfish  
[Table 21](#) lists the default ciphers used for SSHv1:

**Table 21 SSHv1 Default Ciphers**

Cipher index value	Cipher name
200	3des
205	blowfish
210	des



**Note:** blowfish and des are not permitted in FIPS-140-2 mode.

- 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  
[Table 22](#) lists the default ciphers used for SSHv2:

**Table 22**      **SSHv2 Default Ciphers**

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



**Note:** blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc are not permitted in FIPS-140-2 mode.

## client-mac-list

- Syntax**      **client-mac-list**
- Context**      config>system>security>ssh
- Description**      This command enables the context to configure SSH MAC algorithms for SR OS as a client.

## mac

- Syntax**      **mac** *index name mac-name*  
                **no mac** *index*
- Context**      config>system>security>ssh>client-mac-list  
                config>system>security>ssh>server-mac-list
- Description**      This command allows the user to configure SSH MAC algorithms for SR OS as an SSH server or an SSH client.

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

- Default** no mac *index*
- Parameters** *index* — Specifies the index of the algorithm in the list.
- Values** 1 to 255
- mac-name* — Specifies the algorithm for performing encryption or decryption.
- Values** [Table 23](#) lists the default client/server algorithms used for SSHv2.

**Table 23 SSHv2 Default client/server algorithms**

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

## key-re-exchange

- Syntax** **key-re-exchange**
- Context** config>system>security>ssh
- Description** This command enables the key re-exchange context.

## client

- Syntax** **client**
- Context** config>system>security>ssh>key-re-exchange
- Description** This command enables the key re-exchange context for SR OS as an SSH client.

---

## mbytes

<b>Syntax</b>	<b>mbytes</b> { <i>mbytes</i>   <b>disable</b> } <b>no mbytes</b>				
<b>Context</b>	config>system>security>ssh>key-re-exchange>client config>system>security>ssh>key-re-exchange>server				
<b>Description</b>	<p>This command configures the maximum bytes to be transmitted before a key re-exchange is initiated by the server.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>				
<b>Default</b>	mbytes 1024				
<b>Parameters</b>	<p><i>mbytes</i> — Specifies the number of megabytes, on a SSH session, after which the SSH client initiates the key-re-exchange.</p> <table><tr><td><b>Values</b></td><td>1 to 64000</td></tr><tr><td><b>Default</b></td><td>1024</td></tr></table> <p><b>disable</b> — Specifies that a session will never timeout. To re-enable <b>mbytes</b>, enter the command without the <b>disable</b> option.</p>	<b>Values</b>	1 to 64000	<b>Default</b>	1024
<b>Values</b>	1 to 64000				
<b>Default</b>	1024				

## minutes

<b>Syntax</b>	<b>minutes</b> { <i>minutes</i>   <b>disable</b> } <b>no minutes</b>				
<b>Context</b>	config>system>security>ssh>key-re-exchange>client config>system>security>ssh>key-re-exchange>server				
<b>Description</b>	<p>This command configures the maximum time, in minutes, before a key re-exchange is initiated by the server.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>				
<b>Default</b>	minutes 60				
<b>Parameters</b>	<p><i>minutes</i> — Specifies the time interval, in minutes, after which the SSH client will initiate the</p> <p>key-re-exchange.</p> <table><tr><td><b>Values</b></td><td>1 to 1440</td></tr><tr><td><b>Default</b></td><td>60</td></tr></table> <p><b>disable</b> — Specifies that a session will never timeout. To re-enable <b>minutes</b>, enter the command without the <b>disable</b> option.</p>	<b>Values</b>	1 to 1440	<b>Default</b>	60
<b>Values</b>	1 to 1440				
<b>Default</b>	60				



---

## shutdown

<b>Syntax</b>	<b>shutdown</b> <b>no shutdown</b>
<b>Context</b>	config>system>security>ssh>key-re-exchange>client config>system>security>ssh>key-re-exchange>server
<b>Description</b>	This command stops the key exchange. It sets the minutes and bytes to infinity so there will not be any key exchange during the PDU transmission.
<b>Default</b>	no shutdown

## server

<b>Syntax</b>	<b>server</b>
<b>Context</b>	config>system>security>ssh>key-re-exchange
<b>Description</b>	This command enables the key re-exchange context for the SSH server.

## preserve-key

<b>Syntax</b>	<b>[no] preserve-key</b>
<b>Context</b>	config>system>security>ssh
<b>Description</b>	<p>After enabling this command, private keys, public keys, and host key file are saved by the server. It is restored following a system reboot or the ssh server restart.</p> <p>The <b>no</b> form of the command specifies that the keys are held in memory by an SSH server and is not restored following a system reboot.</p>
<b>Default</b>	no preserve-key

## server-cipher-list

<b>Syntax</b>	<b>server-cipher-list protocol-version <i>version</i></b>
<b>Context</b>	config>system>security>ssh
<b>Description</b>	This command enables the configuration of 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 only accepts connections from clients that support SSH protocol version 1 2 — Specifies that the SSH server accepts connections from clients supporting either SSH protocol version 2

## server-mac-list

<b>Syntax</b>	<b>server-mac-list</b>
<b>Context</b>	config>system>security>ssh
<b>Description</b>	This command allows the user to configure SSH MAC algorithms for SR OS as an SSH server.

## 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> <b>no version</b>
<b>Context</b>	config>system>security>ssh
<b>Description</b>	This command configures the SSH protocol version that will be supported by the SSH server.  The <b>no</b> form of the command removes the SSH version from the configuration.
<b>Parameters</b>	<i>ssh-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 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.



**Note:** Values “1” and “1-2” are not permitted in FIPS-140-2 mode.

**Default** 2

## 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 shut down 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>

## telnet6-server

<b>Syntax</b>	<b>[no] telnet6-server</b>
<b>Context</b>	config>system>security
<b>Description</b>	<p>This command enables Telnet IPv6 servers running on the system and only applies to the 7750 SR and 7950 XRS.</p> <p>Telnet servers are shut down by default. At system startup, only SSH servers are enabled.</p> <p>The <b>no</b> form of the command disables Telnet IPv6 servers running on the system.</p>

## vprn-network-exceptions

<b>Syntax</b>	<b>vprn-network-exceptions</b> <i>number seconds</i> <b>no vprn-network-exceptions</b>
<b>Context</b>	config>system>security
<b>Description</b>	<p>This command configures the rate to limit ICMP replies to packets with label TTL expiry received within all VPRN sentences in the system and from all network IP interfaces. This includes labeled user packets, ping and traceroute packets within VPRN.</p>

This feature currently also limits the same packets when received within the context of an LSP shortcut.

This feature does not rate limit MPLS and service OAM packets (vprn-ping, vprn-trace, lsp-ping, lsp-trace, vccv-ping, and vccv-trace).

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

This feature only applies to the 7750 SR and 7950 XRS.

<b>Parameters</b>	<i>number</i> — Specifies the number limit of MPLS exception messages.
	<b>Values</b> 10 to 10,000
	<i>seconds</i> — Specifies the rate limit of MPLS exception messages, in seconds.
	<b>Values</b> 1 to 60

### 2.8.2.3 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>
	<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.
	The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no message-fast-tx
<b>Parameters</b>	<i>time</i> — Specifies the fast transmission period in seconds.
	<b>Values</b> 1 to 3600
	<b>Default</b> 1

---

## message-fast-tx-init

<b>Syntax</b>	<b>message-fast-tx-init</b> <i>count</i> <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.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no message-fast-tx-init
<b>Parameters</b>	<i>count</i> — Specifies the number of LLDPDUs to send during the fast transmission period.  <b>Values</b> 1 to 8 <b>Default</b> 4

## notification-interval

<b>Syntax</b>	<b>notification-interval</b> <i>time</i> <b>no notification-interval</b>
<b>Context</b>	config>system>lldp
<b>Description</b>	This command configures the minimum time between change notifications.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no notification-interval
<b>Parameters</b>	<i>time</i> — Specifies the minimum time, in seconds, between change notifications.  <b>Values</b> 5 to 3600 <b>Default</b> 5

## reinit-delay

<b>Syntax</b>	<b>reinit-delay</b> <i>time</i> <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.  The <b>no</b> form of the command reverts to the default value.

---

<b>Default</b>	no reinit-delay
<b>Parameters</b>	<i>time</i> — Specifies the time, in seconds, before re-initializing LLDP on a port.
<b>Values</b>	1 to 10
<b>Default</b>	2

## tx-credit-max

<b>Syntax</b>	<b>tx-credit-max</b> <i>count</i> <b>no tx-credit-max</b>
<b>Context</b>	config>system>lldp
<b>Description</b>	This command configures the maximum consecutive LLDPDUs transmitted.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no tx-credit-max
<b>Parameters</b>	<i>count</i> — Specifies the maximum consecutive LLDPDUs transmitted.
<b>Values</b>	1 to 100
<b>Default</b>	5

## tx-hold-multiplier

<b>Syntax</b>	<b>tx-hold-multiplier</b> <i>multiplier</i> <b>no tx-hold-multiplier</b>
<b>Context</b>	config>system>lldp
<b>Description</b>	This command configures the multiplier of the tx-interval.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no tx-hold-multiplier
<b>Parameters</b>	<i>multiplier</i> — Specifies the multiplier of the tx-interval.
<b>Values</b>	2 to 10
<b>Default</b>	4

## tx-interval

<b>Syntax</b>	<b>tx-interval</b> <i>interval</i>
---------------	------------------------------------

### **no tx-interval**

<b>Context</b>	config>system>lldp
<b>Description</b>	This command configures the LLDP transmit interval time.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	no tx-interval
<b>Parameters</b>	<i>interval</i> — Specifies the LLDP transmit interval time.
<b>Values</b>	5 to 32768
<b>Default</b>	30

## **2.8.2.4 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>	This command creates the context to edit management access filters and to reset match criteria.  Management access filters control all traffic in and out of the CPM. They can be used to restrict management of the router by other nodes outside either specific (sub)networks or through designated ports.  Management filters, as opposed to other traffic filters, are enforced by system software.  The <b>no</b> form of the command removes management access filters from the configuration.

### **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.

### **ipv6-filter**

<b>Syntax</b>	<b>[no] ipv6-filter</b>
---------------	-------------------------

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

**Description** This command enables the context to configure management access IPv6 filter parameters. This command only applies to the 7750 SR and 7950 XRS.

## mac-filter

**Syntax** [no] mac-filter

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

**Description** This command configures a management access MAC-filter.

## default-action

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

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

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

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

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

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

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

The **deny-host-unreachable** only applies to ip-filter and ipv6filter.

## entry

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

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



<b>Description</b>	<p>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 <i>entry-id</i> 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.</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> defined to be considered complete. Entries without the <b>action</b> keyword are considered incomplete and inactive.</p> <p>The <b>no</b> form of the command removes the specified entry from the management access filter.</p>
<b>Default</b>	No entries are defined.
<b>Parameters</b>	<p><i>entry-id</i> — Specifies 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.</p> <p><b>Values</b>      1 to 9999</p>

## action

<b>Syntax</b>	<b>action {permit   deny   deny-host-unreachable}</b> <b>no action</b>
<b>Context</b>	<pre>config&gt;system&gt;security&gt;mgmt-access-filter&gt;ip-filter&gt;entry config&gt;system&gt;security&gt;mgmt-access-filter&gt;ipv6-filter&gt;entry config&gt;system&gt;security&gt;mgmt-access-filter&gt;mac-filter&gt;entry</pre>
<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> <p>If the packet does not meet any of the match criteria the configured <b>default action</b> is applied.</p>
<b>Parameters</b>	<p><b>permit</b> — 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>The <b>deny-host-unreachable</b> parameter only applies to ip-filter and ipv6-filter.</p>

## dst-port

<b>Syntax</b>	<b>dst-port</b> <i>value</i> [ <i>mask</i> ]
---------------	--

**no dst-port**

- Context**  
config>system>security>mgmt-access-filter>ip-filter>entry  
config>system>security>mgmt-access-filter>ipv6-filter>entry
- Description**  
This command configures a source TCP or UDP port number or port range for a management access filter match criterion.  
  
The **no** form of the command removes the source port match criterion.
- Parameters**  
*value* — Specifies the source TCP or UDP port number as match criteria.  
**Values** 1 to 65535 (decimal)  
*mask* — Specifies the mask used to specify a range of source port numbers as the match criterion.  
This 16 bit mask can be configured using the formats described in [Table 24](#):

**Table 24** Format Styles to Configure Mask

Format Style	Format Syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBB BB	0b1111100000000000

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

- Default** 65535 (exact match)
- Values** 1 to 65535 (decimal)

log

- Syntax** [no] log
- Context**  
config>system>security>mgmt-access-filter>ip-filter>entry  
config>system>security>mgmt-access-filter>ipv6-filter>entry  
config>system>security>mgmt-access-filter>mac-filter>entry
- Description**  
This command enables match logging. When enabled, matches on this entry will cause the Security event mafEntryMatch to be raised.
- Default** no log

## protocol

<b>Syntax</b>	<b>protocol</b> <i>protocol-id</i> <b>no protocol</b>
<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>	<p><i>protocol</i> — Specifies the protocol number for the match criterion.</p> <p><b>Values</b> 1 to 255 (decimal)</p>

## flow-label

<b>Syntax</b>	<b>flow-label</b> <i>value</i> <b>no flow-label</b>
<b>Context</b>	config>system>security>mgmt-access-filter>ipv6-filter>entry
<b>Description</b>	<p>This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service. This command only applies to the 7750 SR and 7950 XRS.</p>
<b>Parameters</b>	<p><i>value</i> — Specifies the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, <i>Textual Conventions for IPv6 Flow Label</i>.)</p> <p><b>Values</b> 0 to 1048575</p>

## next-header

<b>Syntax</b>	<b>next-header</b> <i>next-header</i> <b>no next-header</b>
<b>Context</b>	config>system>security>mgmt-access-filter>ipv6-filter>entry
<b>Description</b>	<p>This command specifies the next header to match. The protocol type such as TCP, UDP or OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17). IPv6 Extension headers are identified by the next header IPv6 numbers as per RFC2460. This command only applies to the 7750 SR and 7950 XRS.</p>

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

**Values**

next-header: 0 to 255, protocol numbers accepted in DHB

keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, drp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, spf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

## router

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

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

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

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

**Parameters** *router-instance* — Specifies one of the following parameters for the router instance:  
*router-name* — Specifies a router name or CPM router instance, up to 32 characters to be used in the match criteria.

**Values** “Base” | “management” | “vpls-management”  
**Default** Base

*vprn-svc-id* — Specifies a CPM router instance to be used in the match criteria

**Values** 1 to 2147483647

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

## src-ip

**Syntax** **src-ip {ip-prefix/mask | ip-prefix netmask}**  
**no src-ip**

**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.

<b>Default</b>	No source IP match criterion is specified.
<b>Parameters</b>	<p><i>ip-prefix</i> — Specifies the IP prefix for the IP match criterion in dotted decimal notation.</p> <p><i>mask</i> — Specifies the subnet mask length expressed as a decimal integer.</p> <p><b>Values</b> 1 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)</p> <p><i>netmask</i> — Specifies the dotted quad equivalent of the mask length.</p> <p><b>Values</b> 0.0.0.0 to 255.255.255.255</p>

## src-ip

<b>Syntax</b>	[no] <b>src-ip</b> { <i>ipv6-address</i>   <i>prefix-length</i> }				
<b>Context</b>	config>system>security>mgmt-access-filter>ipv6-filter>entry				
<b>Description</b>	<p>This command configures a source IPv6 address range prefix to be used as a management access filter match criterion. This command only applies to the 7750 SR and 7950 XRS.</p> <p>The <b>no</b> form of the command removes the source IPv6 address match criterion.</p>				
<b>Default</b>	No source IP match criterion is specified.				
<b>Parameters</b>	<p><i>ipv6-address/prefix-length</i> — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:217A.</p> <p><b>Values</b></p> <table> <tr> <td><i>ipv6-address</i></td><td> x:x:x:x:x:x:x:x (eight 16-bit pieces)  x:x:x:x:x:d.d.d.d  x: [0..FFFF]H  d: [0..255]D </td></tr> <tr> <td><i>prefix-length</i></td><td>1 to 128</td></tr> </table>	<i>ipv6-address</i>	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0..FFFF]H d: [0..255]D	<i>prefix-length</i>	1 to 128
<i>ipv6-address</i>	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0..FFFF]H d: [0..255]D				
<i>prefix-length</i>	1 to 128				

## src-port

<b>Syntax</b>	<b>src-port</b> { <i>port-id</i>   <b>cpm</b>   <b>lag</b> <i>lag-id</i> } <b>no src-port</b>
<b>Context</b>	config>system>security>mgmt-access-filter>ip-filter>entry config>system>security>mgmt-access-filter>ipv6-filter>entry
<b>Description</b>	This command restricts ingress management traffic to either the CPM/CCM 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.

<b>Default</b>	any interface
<b>Parameters</b>	<i>port-id</i> — Specifies the port ID in formats shown below
	<b>Values</b>
	<i>slot/mda/port[.channel]</i>
	<i>bundle-id</i> <b>bundle-type-slot/mda.bundle-num</b>
	<b>bundle</b> keyword
	<i>type</i> <b>ima, fr, or ppp</b>
	<i>bundle-num</i> 1 to 336
	<i>bpgrp-id</i> <b>bpgrp-type-bpgrp-num</b>
	<b>bpgrp</b> keyword
	<i>type</i> <b>ima or ppp</b>
	<i>bpgrp-num</i> 1 to 2000
	<i>aps-id</i> <b>aps-group-id[.channel]</b>
	<b>aps</b> keyword
	<i>group-id</i> 1 to 128
	<i>ccag-id</i> <b>ccag-id. path-id[cc-type]</b>
	<b>ccag</b> keyword
	<i>id</i> 1 to 8
	<i>path-id</i> <b>a, b</b>
	<i>cc-type</i> <b>.sap-net, .net-sap</b>

**cpm** — Matches any traffic received on any Ethernet port

*lag-id* — Specifies the LAG identifier

**Values**      1 to 800

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

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

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

**Values** 1 to 9999

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

**Values** 1 to 9999

## shutdown

**Syntax** [no] shutdown

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

**Description** This command disables the management-access-filter.

## match

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

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

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

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

**Values** 802dot3 | 802dot2-llc | 802dot2-snap | 802dot1ag | ethernet\_II

**Default** 802dot3

## cfm-opcode

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

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

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

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

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

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

Table 25 lists the opcode values.

**Table 25 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



**Table 25 Opcode Values (Continued)**

CFM PDU or Organization	Acronym	Configurable Numeric Value (Range)
	1DM	45
	DMR	46
	DMM	47
Reserved for ITU		48 – 63
Reserved for IEEE 802.1 0		64 - 255

Defined by ITU-T Y.1731 32 - 63

Defined by IEEE 802.1.64 - 255

**Default** no cfm-opcode

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

*start* — specifies the start number.

**Values** 0 to 255

*end* — Specifies the end number.

**Values** 0 to 255

**lt | gt | eq** — Specifies comparison operators.

## 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.

**Table 26 Management Access Filter dot1p Mask Format**

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

**Parameters**    *dot1p-value* — Specifies the IEEE 802.1p value in decimal.  
                  **Values**        0 to 7  
*mask* — Specifies the 3-bit mask can be configured using the following formats.

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.  
**Parameters**    *dsap-value* — Specifies the 8-bit DSAP match criteria value in hexadecimal.  
                  **Values**        0x00 to 0xFF (hex)  
*mask* — Specifies a range of DSAP values to use as the match criteria.  
                  This 8 bit mask can be configured using the formats described in [Table 27](#):

**Table 27        Format Styles**

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

**Default**        FF (hex) (exact match)  
**Values**        0x00 to 0xFF

dst-mac

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

## etype

<b>Syntax</b>	<b>etype</b> <i>0x0600xx0xffff</i> <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 <i>7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide</i> 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> — Specifies the Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.</p> <p><b>Values</b>      0x0600 to 0xFFFF</p>

## snap-oui

<b>Syntax</b>	<b>snap-oui</b> {zero   non-zero} <b>no snap-oui</b>
<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> <b>no snap-pid</b>
<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 PID value to be used as a MAC filter match criterion.</p> <p>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.</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 <i>7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide</i> for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.</p> <div style="border: 1px solid blue; padding: 2px; display: inline-block; vertical-align: middle;">→</div> <p><b>Note:</b> 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.</p> <p>The <b>no</b> form of the command removes the snap-pid value as the match criteria.</p>
<b>Default</b>	no snap-pid
<b>Parameters</b>	<p><i>pid-value</i> — Specifies the two-byte snap-pid value to be used as a match criterion in hexadecimal.</p> <p><b>Values</b>      0x0000 to 0xFFFF</p>

## src-mac

<b>Syntax</b>	<b>src-mac</b> <i>ieee-address</i> [ <i>ieee-address-mask</i> ] <b>no src-mac</b>
<b>Context</b>	config>system>security>mgmt-access-filter>mac-filter>entry>match
<b>Description</b>	<p>This command configures a source MAC address or range to be used as a MAC filter match criterion.</p> <p>The <b>no</b> form of the command removes the source mac as the match criteria.</p>
<b>Default</b>	no src-mac
<b>Parameters</b>	<p><i>ieee-address</i> — Specifies the 48-bit IEEE mac address to be used as a match criterion.</p> <p><b>Values</b>      HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit</p>

*ieee-address-mask* — Specifies a 48-bit mask that can be configured using the formats listed in [Table 28](#):

**Table 28**      **ieee-address-mask Formats**

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHHH	0x0FFFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFFFF000000

**Default**      0xFFFFFFFFFFFFFFF (exact match)  
**Values**      0x000000000000000 to 0xFFFFFFFFFFFFFFF

ssap

- Syntax

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

config>system>security>mgmt-access-filter>mac-filter>entry>match
- Description

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

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

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of the command removes the SSAP match criterion.
- Default

no ssap
- Parameters

*ssap-value* — Specifies the 8-bit SSAP match criteria value in hex.

**Values**      0x00 to 0xFF

*ssap-mask* — Specifies a range of SSAP values to use as the match criteria.

## svc-id

<b>Syntax</b>	<b>svc-id</b> <i>service-id</i> <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>	<i>service-id</i> — Specifies a service-id to match. <b>Values</b> <i>service-id</i> : 1 to 2147483647 <i>svc-name</i> : 64 characters maximum

## 2.8.2.5 CLI Script Authorization 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.

### cli-user

<b>Syntax</b>	<b>cli-user</b> <i>user-name</i>
---------------	----------------------------------

### no cli-user

<b>Context</b>	config>system>security>cli-script>authorization>cron config>system>security>cli-script>authorization>event-handler config>system>security>cli-script>authorization>vsd
<b>Description</b>	<p>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 <b>cli-script</b> authorization.</p> <p>The <b>no</b> form of this command configures scripts to execute with no restrictions and without performing authorization.</p>
<b>Default</b>	no cli-user
<b>Parameters</b>	<i>user-name</i> — 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.

## event-handler

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

## vsd

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

## 2.8.2.6 CPM Filter Commands

### cpm-filter

<b>Syntax</b>	<b>cpm-filter</b>
---------------	-------------------

---

**Context** config>system>security

**Description** This command enables the context to configure a CPM filter. A CPM filter is a hardware filter done by the P chip on the CPM and CFM that applies to all the traffic going to the CPM or CFM CPU. It can be used to drop, accept packets, as well as allocate dedicated hardware queues for the traffic.

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

## default-action

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

**Context** config>system>security>cpm-filter

**Description** This command specifies the action to take on the traffic when the filter entry matches. If there are no filter entry defined, the packets received will either be dropped or forwarded based on that default action.

**Default** default-action accept

**Parameters** **accept** — Specifies that packets matching the filter entry are forwarded.  
**drop** — Specifies that packets matching the filter entry are dropped.

## ip-filter

**Syntax** [no] ip-filter

**Context** config>system>security>cpm-filter

**Description** This command enables the context to configure CPM IP filter parameters.

**Default** shutdown

## ipv6-filter

**Syntax** [no] ipv6-filter

**Context** config>system>security>cpm-filter

**Description** This command enables the context to configure CPM IPv6 filter parameters. This command applies only to the 7750 SR and 7950 XRS.

**Default** shutdown



## 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 <i>entry-id</i></b>		
<b>Context</b>	config>sys>sec>cpm>ip-filter config>sys>sec>cpm>ipv6-filter 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.  The default match criteria is match none.		
<b>Parameters</b>	<i>entry-id</i> — Identifies a CPM filter entry as configured on this system.  <table> <tr> <td><b>Values</b></td><td>1 to 6144 for ip-filter and ipv6-filter 1 to 2048 for mac-filter</td></tr> </table>	<b>Values</b>	1 to 6144 for ip-filter and ipv6-filter 1 to 2048 for mac-filter
<b>Values</b>	1 to 6144 for ip-filter and ipv6-filter 1 to 2048 for mac-filter		

## action

<b>Syntax</b>	<b>action [accept   drop   queue <i>queue-id</i>] no action</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry config>sys>sec>cpm>ipv6-filter>entry config>sys>sec>cpm>mac-filter>entry
<b>Description</b>	This command specifies the action to take for packets that match this filter entry.
<b>Default</b>	action drop
<b>Parameters</b>	<b>accept</b> — Specifies packets matching the entry criteria will be forwarded. <b>drop</b> — Specifies packets matching the entry criteria will be dropped. <b>queue <i>queue-id</i></b> — Specifies packets matching the entry criteria will be forward to the specified CPM hardware queue.

---

## log

<b>Syntax</b>	<b>log</b> <i>log-id</i>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry config>sys>sec>cpm>ipv6-filter>entry 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.  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> ] <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 <b>match</b> context may consist of multiple match criteria, but multiple <b>match</b> statements cannot be entered per entry.  The <b>no</b> form of the command removes the match criteria for the <i>entry-id</i> .
<b>Parameters</b>	<b>protocol</b> — 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.  <i>protocol-id</i> — 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 <b>no</b> form the command removes the protocol from the match criteria.  <b>Values</b> 1 to 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 29 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	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol

**Table 29 IP Protocol Names (Continued)**

Protocol	Protocol ID	Description
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

## match

- Syntax** **match** [*next-header next-header*]  
**no match**
- Context** config>sys>sec>cpm>ipv6-filter>entry
- Description** This command specifies match criteria for the IP filter entry. This command applies only the 775 SR and 7950 XRS.
- The **no** form of this command removes the match criteria for the *entry-id*.
- Parameters** *next-header* — Specifies the next header to match.
- The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).
- Values**
- next-header: 1 to 42, 45 to 49, 52 to 59, 61 to 255 protocol numbers accepted in DHB
  - keywords: none, crt, crudp, ecp, eigrp, encap, ether-ip, gre, icmp, drp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, spf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
  - \* — udp/tcp wildcard

## dscp

- Syntax** **dscp** *dscp-name*  
**no dscp**
- Context** config>sys>sec>cpm>ip-filter>entry>match  
config>sys>sec>cpm>ipv6-filter>entry>match  
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.  The <b>no</b> form of the command removes the DSCP match criterion.
<b>Default</b>	no dscp
<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>ip-address/mask</i> <b>dst-ip</b> <i>ip-address netmask</i> <b>dst-ip ip-prefix-list</b> <i>ip-prefix-list-name</i> <b>no dst-ip</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry>match config>sys>sec>cpm>ipv6-filter>entry>match
<b>Description</b>	This command configures a destination IP address range to be used as an IP filter match criterion.  To match on the destination IP address, specify the address and its associated mask, for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.  The <b>no</b> form of the command removes the destination IP address match criterion.
<b>Default</b>	no dst-ip
<b>Parameters</b>	<i>ip-address</i> — Specifies the IP address for the IP match criterion in dotted decimal notation.  <b>Values</b> 0.0.0.0 to 255.255.255.255  <b>ip-prefix-list</b> — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.  <i>ip-prefix-list-name</i> — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.  <i>mask</i> — Specifies the subnet mask length expressed as a decimal integer.  <b>Values</b> 1 to 32  <i>netmask</i> — Specifies the dotted quad equivalent of the mask length.  <b>Values</b> 0.0.0.0 to 255.255.255.255

## dst-ip

<b>Syntax</b>	<b>dst-ip</b> [ <i>ipv6-address /prefix-length</i> ] [ <b>ipv6-prefix-list</b> <i>ipv6-prefix-list-name</i> ] <b>no dst-ip</b>										
<b>Context</b>	config>sys>sec>cpm>ipv6-filter>entry>match										
<b>Description</b>	<p>This command configures a destination IPv6 address range to be used as an IPv6 filter match criterion.</p> <p>To match on the destination IPv6 address, specify the address.</p> <p>The <b>no</b> form of the command removes the destination IP address match criterion.</p> <p>This command only applies to the 7750 SR and 7950 XRS.</p>										
<b>Default</b>	no dst-ip										
<b>Parameters</b>	<p><i>ipv6-address/prefix-length</i> — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:217A.</p> <p><b>Values</b></p> <table> <tr> <td>x:x:x:x:x:x:x</td><td>(eight 16-bit pieces)</td></tr> <tr> <td>x:x:x:x:x:d.d.d.d</td><td></td></tr> <tr> <td>x:</td><td>[0 to .FFFF]H</td></tr> <tr> <td>d:</td><td>[0 to 255]D</td></tr> <tr> <td>prefix-length:</td><td>1 to 128</td></tr> </table> <p><b>ipv6-prefix-list</b> — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.</p> <p><i>ipv6-prefix-list-name</i> — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.</p>	x:x:x:x:x:x:x	(eight 16-bit pieces)	x:x:x:x:x:d.d.d.d		x:	[0 to .FFFF]H	d:	[0 to 255]D	prefix-length:	1 to 128
x:x:x:x:x:x:x	(eight 16-bit pieces)										
x:x:x:x:x:d.d.d.d											
x:	[0 to .FFFF]H										
d:	[0 to 255]D										
prefix-length:	1 to 128										

## dst-port

<b>Syntax</b>	<b>dst-port</b> [ <i>tcp/udp port-number</i> ] [ <i>mask</i> ] <b>dst-port port-list</b> <i>port-list-name</i> <b>dst-port range</b> <i>tcp/udp port-number tcp/udp port-number</i> <b>no dst-port</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry>match config>sys>sec>cpm>ipv6-filter>entry>match

**Description** This command specifies the TCP/UDP port or port name to match the destination-port of the packet.



**Note:** 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.

**Default** no dst-port

**Parameters** *tcp/udp port-number* — Specifies the destination port number to be used as a match criteria expressed as a decimal integer.

**Values** 0 to 65535 (accepted in decimal hex or binary)

*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 to 0xFFFF] | [0 to 65535] | [0b0000000000000000 to 0b1111111111111111]

## flow-label

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

**Context** config>sys>sec>cpm>ipv6-filter>entry>match

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

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

**Values** 0 to 1048575

## fragment

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

**Context** config>sys>sec>cpm>ip-filter>entry>match  
config>sys>sec>cpm>ipv6-filter>entry>match

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



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

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.

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

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.

**Default** no fragment

**Parameters** **true** — Specifies to match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value. For IPv6, packet matches if it contains IPv6 Fragmentation Extension Header.

**false** — Specifies to match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero. For IPv6, packet matches if it does not contain IPv6 Fragmentation Extension Header.

## hop-by-hop-opt

**Syntax** **hop-by-hop-opt {true | false}**  
**no hop-by-hop-opt**

**Context** config>sys>sec>cpm>ipv6-filter>entry>match

**Description** This command enables match on existence of Hop-by-Hop Options Extension Header in the IPv6 filter policy. This command applies to the 7750 SR and 7950 XRS.

The **no** form of this command ignores Hop-by-Hop Options Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

**Default** no hop-by-hop-opt



- Parameters**     **true** — Match if a packet contains Hop-by-Hop Options Extension Header.  
                       **false** — Match if a packet does not contain Hop-by-Hop Options Extension Header.

## icmp-code

- Syntax**     **icmp-code** *icmp-code*  
                  **no icmp-code**
- Context**     config>sys>sec>cpm>ip-filter>entry>match  
                  config>sys>sec>cpm>ipv6-filter>entry>match
- Description**     This command configures matching on ICMP code field in the ICMP header of an IP packet as an IP filter match criterion.



**Note:** 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 behavior of the **icmp-code** value is dependent on the configured **icmp-type** value, thus a configuration with only an **icmp-code** value specified will have no effect. To match on the **icmp-code**, an associated **icmp-type** must also be specified.

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

- Default**     no icmp-code
- Parameters**     *icmp-code* — Specifies the ICMP code values that must be present to match.  
                       **Values**     0 to 255

## icmp-type

- Syntax**     **icmp-type** *icmp-type*  
                  **no icmp-type**
- Context**     config>sys>sec>cpm>ip-filter>entry>match  
                  config>sys>sec>cpm>ipv6-filter>entry>match
- Description**     This command configures matching on ICMP type field in the ICMP header of an IP packet as an IP filter match criterion.



**Note:** 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 criterion from the match entry.

**Default** no icmp-type

**Parameters** *icmp-type* — Specifies the ICMP type values that must be present to match.

**Values** 0 to 255

ip-option

**Syntax** **ip-option** *ip-option-value ip-option-mask*  
**no ip-option**

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

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

The option-type octet contains 3 fields:

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

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

**Default** no ip-option

**Parameters** *ip-option-value* — Enter the 8 bit option-type as a decimal integer. The mask is applied as an AND to the option byte, the result is compared with the option-value.  
The decimal value entered for the match should be a combined value of the eight bit option type field and not just the option number. Thus to match on IP packets that contain the Router Alert option (option number =20), enter the option type of 148 (10010100).

**Values** 0 to 255

*ip-option-mask* — Specifies a range of option numbers to use as the match criteria.  
This 8 bit mask can be configured using the formats described in [Table 30](#):

**Table 30** ip-option-mask Formats

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0xHH	0x14
Binary	0BBBBBBBBB	0b0010100

**Default** 255 (decimal) (exact match)

**Values** 1 to 255 (decimal)

## multiple-option

**Syntax** **multiple-option {true | false}**  
**no multiple-option**

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

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

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

**Default** no multiple-option

**Parameters** **true** — Specifies matching on IP packets that contain more than one option field in the header.

**false** — Specifies matching on IP packets that do not contain multiple option fields present in the header.

## option-present

**Syntax** **option-present {true | false}**  
**no option-present**

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

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

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

**Default** no option-present

**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.

## port

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

**Context** config>system>security>cpm-filter>ip-filter>entry>match  
 config>system>security>cpm-filter>ipv6-filter>entry>match

**Description** 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.

This command is mutually exclusive with **src-port** and **dst-port** commands.

The **no** form of this command deletes the specified port match criterion.

**Default** no port

**Parameters** *tcp/udp port-number* — Specifies the source or destination port to be used as a match criterion specified as a decimal integer.

**Values** 0 to 65535

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

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

**range** *tcp/udp port-number* — Specifies 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 to 65535

**port-list** *port-list-name* — Specifies 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 service-name</b> <i>service-name</i> <b>router</b> <i>router-instance</i> <b>no router</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry>match config>sys>sec>cpm>ipv6-filter>entry>match
<b>Description</b>	This command specifies a router name or a service-id to be used in the match criteria.
<b>Default</b>	no router
<b>Parameters</b>	<i>router-instance</i> — Specifies one of the following parameters for the router instance: <i>router-name</i> — Specifies a router name up to 32 characters to be used in the match criteria. <i>service-id</i> — Specifies an existing service ID to be used in the match criteria. <b>Values</b> 1 to 2147483647 <i>service-name service-name</i> — Specifies an existing service name up to 64 characters in length.

## src-ip

<b>Syntax</b>	<b>src-ip</b> [ <i>ipv6-address/prefix-length</i> ] <b>ip-prefix-list</b> <i>prefix-list-name</i> <b>no src-ip</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter>entry>match
<b>Description</b>	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 <b>no</b> form of the command removes the source IP address match criterion.
<b>Default</b>	no src-ip
<b>Parameters</b>	<i>ipv6-address/prefix-length</i> — 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 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A. <b>Values</b> <i>ipv4-address</i> a.b.c.d (host bits must be 0) x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D

interface: 32 characters maximum, mandatory for link local addresses

*prefix-length*      1 to 128

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

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

src-ip

<b>Syntax</b>	<b>src-ip</b> [ <i>ip-address/mask</i>   <b>ipv6-prefix-list</b> <i>ipv6-prefix-list-name</i> ] <b>no src-ip</b>						
<b>Context</b>	config>sys>sec>cpm>ipv6-filter>entry>match						
<b>Description</b>	<p>This command specifies the IPv6 address to match the source IPv6 address of the packet.</p> <p>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.</p> <p>The <b>no</b> form of the command removes the source IP address match criterion.</p> <p>This command only applies to the 7750 SR and 7950 XRS.</p>						
<b>Default</b>	no src-ip						
<b>Parameters</b>	<p><i>ip-address/mask</i> — 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 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A.</p> <p><b>Values</b></p> <table><tr><td>ipv6-address</td><td>x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses</td></tr><tr><td>mask:</td><td>Specifies eight 16-bit hexadecimal pieces representing bit match criteria.</td></tr><tr><td>Values</td><td>x:x:x:x:x:x (eight 16-bit pieces)</td></tr></table>	ipv6-address	x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses	mask:	Specifies eight 16-bit hexadecimal pieces representing bit match criteria.	Values	x:x:x:x:x:x (eight 16-bit pieces)
ipv6-address	x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses						
mask:	Specifies eight 16-bit hexadecimal pieces representing bit match criteria.						
Values	x:x:x:x:x:x (eight 16-bit pieces)						

**ipv6-prefix-list** — Creates a list of IPv6 prefixes for match criteria in IPv6 ACL and CPM filter policies.

*ipv6-prefix-list-name* — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

## src-port

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

**Context** config>sys>sec>cpm>ip-filter>entry>match  
config>sys>sec>cpm>ipv6-filter>entry>match

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



**Note:** 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.

**Default** no src-port

**Parameters** *tcp/udp port-number* — Specifies the source port number to be used as a match criteria expressed as a decimal integer.

**Values** 0 to 65535

*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]

## tcp-ack

**Syntax** **tcp-ack** {true | false}  
**no tcp-ack**

**Context** config>sys>sec>cpm>ip-filter>entry>match  
config>sys>sec>cpm>ipv6-filter>entry>match

**Description** This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion.



**Note:** 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 criterion from the match entry.

**Default** no tcp-ack

**Parameters** **true** — Specifies matching on IP or IPv6 packets that have the ACK bit set in the control bits of the TCP header of an IP or IPv6 packet.

**false** — Specifies matching on IP or IPv6 packets that do not have the ACK bit set in the control bits of the TCP header of the IP or IPv6 packet.

## tcp-syn

**Syntax** **tcp-syn {true | false}**  
**no tcp-syn**

**Context** config>sys>sec>cpm>ip-filter>entry>match  
config>sys>sec>cpm>ipv6-filter>entry>match

**Description** This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion.



**Note:** 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 tcp-syn

**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

<b>Syntax</b>	<b>renum</b> <i>old-entry-id</i> <i>new-entry-id</i>
<b>Context</b>	config>sys>sec>cpm>ip-filter config>sys>sec>cpm>ipv6-filter config>sys>sec>cpm>mac-filter
<b>Description</b>	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.
<b>Parameters</b>	<i>old-entry-id</i> — Specifies the entry number of an existing entry.  <b>Values</b> 1 to 6144 for ip-filter and ipv6-filter 1 to 2048 for mac-filter  <i>new-entry-id</i> — Specifies the new entry number to be assigned to the old entry.  <b>Values</b> 1 to 6144 for ip-filter and ipv6-filter 1 to 2048 for mac-filter

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>sys>sec>cpm>ip-filter config>sys>sec>cpm>ipv6-filter config>sys>sec>cpm>mac-filter
<b>Description</b>	This command enables IPv4, IPv6 or MAC CPM filter.  The <b>no</b> form of this command disable the filter.
<b>Default</b>	shutdown

### 2.8.2.7 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>create</b> ]
<b>Context</b>	config>system>security>cpm-queue
<b>Description</b>	This command allows users to allocate dedicated CPM. The first available queue is 33.
<b>Parameters</b>	<i>queue-id</i> — 33 to 2000

## cbs

<b>Syntax</b>	<b>cbs</b> <i>cbs</i> <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> <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> [ <i>cir</i> <i>cir</i> ] <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 (kb/s).

---

**Parameters**     *rate* — Specifies the administrative Peak Information Rate (PIR) for the queue.  
                    *cir* — Specifies the amount of bandwidth committed to the queue.

## 2.8.2.8 CPU Protection Commands

### cpu-protection

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

### included-protocols

**Syntax**        **included-protocols**  
**Context**       config>sys>security>cpu-protection>ip>included-protocols  
**Description**   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

**Syntax**        **[no] dhcp**  
**Context**       config>sys>security>cpu-protection>ip>included-protocols  
**Description**   This command includes the extracted IPv4 DHCP packets for ip-src-monitoring. IPv4 DHCP packets will be subject to the per-source-rate of CPU protection policies.  
**Default**       dhcp (Note this is different from the other protocols)

### gtp

**Syntax**        **[no] gtp**  
**Context**       config>sys>security>cpu-protection>ip>included-protocols  
**Description**   This command includes the extracted IPV4 GTP packets for ip-src-monitoring. IPv4 GTP packets will be subject to the per-source-rate of CPU protection policies.  
**Default**       no gtp

---

## icmp

<b>Syntax</b>	<b>[no] icmp</b>
<b>Context</b>	config>sys>security>cpu-protection>ip>included-protocols
<b>Description</b>	This command includes the 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>	This command includes the 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 <i>packet-rate-limit</i></b> <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>	link-specific-rate 15000
<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 to 65535, <b>max</b> (no limit)

## policy

<b>Syntax</b>	<b>policy <i>cpu-protection-policy-id</i> [create]</b> <b>no policy <i>cpu-protection-policy-id</i></b>
<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> <ul style="list-style-type: none"> <li>• per-source-rate: max (no limit)</li> <li>• overall-rate: 6000</li> <li>• out-profile-rate: 6000</li> <li>• alarm</li> </ul> <p>Policy 255 (default network interface policy):</p> <ul style="list-style-type: none"> <li>• per-source-rate: max (no limit)</li> <li>• overall-rate: max (no limit)</li> <li>• out-profile-rate: 3000</li> <li>• alarm</li> </ul>
<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 to 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>[no] eth-cfm</b>
<b>Context</b>	config>sys>security>cpu-protection>policy

---

**Description** Provides the construct under which the different entries within CPU policy can define the match criteria and overall arrival rate of the Ethernet Configuration and Fault Management (ETH-CFM) packets at the CPU.

## entry

**Syntax** **entry** *entry levels levels opcodes opcodes rate packet-rate-limit*  
**no entry**

**Context** config>sys>security>cpu-protection>eth-cfm>

**Description** Builds the specific match and rate criteria. Up to ten entries may exist in up to four CPU protection policies.

The **no** form of the command reverses the match and rate criteria configured.

**Default** no entry

**Parameters** *rate* — Specifies a packet rate limit in frames per second, where a “0” means drop all.

**Values** 1 to 100

*level* — Specifies a domain level.

**Values** all: Wildcard entry level  
range: 0 to 7: within specified range, multiple ranges allowed  
number: 0 to 7: specific level number, may be combined with range

*opcode* — Specifies an operational code that identifies the application.

**Values** range: 0 to 255: within specified range, multiple ranges allowed  
number: 0 to 255: specific level number, may be combined with range

## out-profile-rate

**Syntax** **out-profile-rate** *packet-rate-limit [log-event]*  
**no out-profile-rate**

**Context** config>sys>security>cpu-protection>policy

**Description** This command applies a packet arrival rate limit for the entire SAP/interface, above which packets will be marked as discard eligible, in other words, out-profile/low-priority/yellow. 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.

The **no** form of the command sets out-profile-rate parameter back to the default value.

---

<b>Default</b>	<p>out-profile-rate 3000 for cpu-protection-policy-id 1-253</p> <p>out-profile-rate 6000 for cpu-protection-policy-id 254 (default access interface policy)</p> <p>out-profile-rate 3000 for cpu-protection-policy-id 255 (default network interface policy)</p>
<b>Parameters</b>	<p><i>packet-rate-limit</i> — Specifies a packet arrival rate limit in packets per second.</p> <p><b>Values</b> 1 to 65535, <b>max</b> (max indicates no limit)</p> <p><b>log-events</b> — Issues a tmnxCpmProtViolSapOutProf, tmnxCpmProtViolIfOutProf, or tmnxCpmProtViolSdpBindOutProf log event and tracks violating interfaces when the out-profile-rate is exceeded. Supported on CPM3 and above only.</p>

## overall-rate

<b>Syntax</b>	<p><b>overall-rate</b> <i>packet-rate-limit</i></p> <p><b>no overall-rate</b></p>
<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>	<p>overall max for cpu-protection-policy-id 1 to 253</p> <p>overall 6000 for cpu-protection-policy-id 254 (default access interface policy)</p> <p>overall max for cpu-protection-policy-id 255 (default network interface policy)</p>
<b>Parameters</b>	<p><i>packet-rate-limit</i> — Specifies a packet arrival rate limit in packets per second.</p> <p><b>Values</b> 1 to 65535, <b>max</b> (the max indicates no limit)</p>

## per-source-rate

<b>Syntax</b>	<p><b>per-source-rate</b> <i>packet-rate-limit</i></p> <p><b>no per-source-rate</b></p>
<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 (mac-monitoring) or SAP and source IP address (ip-src-monitoring). The CPU will receive no more than the configured packet rate from each source (only certain protocols are rate limited for ip-src-monitoring as configured under <b>include-protocols</b> in the <b>cpu-protection</b> 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 saps, subscriber-interfaces, and spoke-sdps), 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 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.</p>
<b>Default</b>	per-source-rate max
<b>Parameters</b>	<p><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.</p> <p><b>Values</b> 1 to 65535, <b>max</b> (max indicates no limit)</p>

## port-overall-rate

<b>Syntax</b>	<b>port-overall-rate</b> <i>packet-rate-limit</i> [ <b>low-action-priority</b> ] <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>Default</b>	port-overall-rate max
<b>Parameters</b>	<p><i>packet-rate-limit</i> — Specifies an overall per-port packet arrival rate limit in packets per second.</p> <p><b>Values</b> 1 to 65535, max (indicates no limit)</p> <p><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.</p>

## protocol-protection

<b>Syntax</b>	<b>protocol-protection</b> [ <b>allow-sham-links</b> ] [ <b>block-pim-tunneled</b> ] <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>	<p><b>allow-sham-links</b> — Allows sham links. As OSPF sham links form an adjacency over the MPLS-VPNRN backbone network, when protocol-protection is enabled, the tunneled OSPF packets to be received over the backbone network must be explicitly allowed.</p> <p><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.</p>

## cpu-protection

<b>Syntax</b>	<b>cpu-protection <i>policy-id</i></b> <b>no cpu-protection</b>
<b>Context</b>	config>router>interface config>service>ies>interface config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>interface config>service>vprn>network-interface config>service>vprn>video-interface
<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>	cpu-protection 254 (for access interfaces) cpu-protection 255 (for network interfaces) no cpu-protection (for video interfaces)

---

## cpu-protection

<b>Syntax</b>	<b>cpu-protection policy-id [mac-monitoring] [ip-src-monitoring]</b> <b>no cpu-protection</b>
<b>Context</b>	config>subscr-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>
<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>ip-src-monitoring</b> — 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.</p>

## cpu-protection

<b>Syntax</b>	<b>cpu-protection policy-id [mac-monitoring]   [eth-cfm-monitoring [aggregate][car]]   [ip-src-monitoring]</b> <b>no cpu-protection</b>
<b>Context</b>	config>service>ies>if>sap config>service>ies>if>spoke-sdp config>service>ies>sub-if>grp-if>sap config>service>vprn>if>sap config>service>vprn>if>spoke-sdp config>service>vprn>sub-if>grp-if>sap

<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>
<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>ip-src-monitoring</b> — 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.</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>

## 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> ]] <b>no cpu-protection</b>
<b>Context</b>	<pre>config&gt;service&gt;epipe&gt;sap config&gt;service&gt;epipe&gt;spoke-sdp config&gt;service&gt;ipipe&gt;sap config&gt;service&gt;template&gt;vpls-sap-template config&gt;service&gt;vpls&gt;mesh-sdp config&gt;service&gt;vpls&gt;sap config&gt;service&gt;vpls&gt;spoke-sdp</pre>
<b>Description</b>	Use this command to apply a specific CPU protection policy to the associated SAP, SDP or template. If the mac-monitoring keyword is given then per MAC rate limiting should be performed, using the per-source-rate from the associated cpu-protection policy.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

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

**Default**    `cpu-protection 254` (for access interfaces)

`cpu-protection 255` (for network interfaces)

The configuration of no `cpu-protection` returns the SAP/SDP/template to the default policies as shown above.

**Parameters**    **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated `cpu-protection` policy.

**eth-cfm-monitoring** — Enables the Ethernet Connectivity Fault Management `cpu-protection` extensions on the associated SAP/SDP/template.

**aggregate** — applies the rate limit to the sum of the per-peer packet rates.

**car** — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.

## 2.8.2.9 Distributed CPU Protection Commands

### dist-cpu-protection

**Syntax**    **dist-cpu-protection**

**Context**    `config>system>security`

**Description**    This command enters the CLI context for configuration of the Distributed CPU Protection (DCP) feature.

### policy

**Syntax**    `[no] policy policy-name`

**Context**    `config>sys>security>dist-cpu-protection`

**Description**    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.

**Parameters**    *policy-name* — Name of the policy to be configured.

## local-monitoring-policer

<b>Syntax</b>	<b>[no] local-monitoring-policer</b> <i>policer-name</i> [ <b>create</b> ]
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>
<b>Description</b>	<p>This command configures a monitoring policer 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 nonconforming 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>policer-name</i> — Specifies name of the policy.
<b>Values</b>	[32 chars max]

## exceed-action

<b>Syntax</b>	<b>exceed-action</b> { <b>discard</b>   <b>low-priority</b>   <b>none</b> }
<b>Context</b>	config>sys>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>Parameters</b>	<p><b>discard</b> — Discards packets that are nonconforming.</p> <p><b>low-priority</b> — Marks packets that are nonconforming as low-priority (discard eligible or out-profile). If there is congestion in the control plane of the SR OS then unmarked (green, hi-prio or in-profile) control packets are given preferential treatment.</p> <p><b>none</b> — no hold-down</p>

## log-events

<b>Syntax</b>	<b>log-events</b> [ <b>verbose</b> ] <b>no log-events</b>
<b>Context</b>	config>sys>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
<b>Parameters</b>	<b>verbose</b> — 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

## rate

<b>Syntax</b>	<b>rate kbps</b> <i>kilobits-per-second</i>   <b>max</b> [ <b>mbs size</b> ] [ <b>bytes</b>   <b>kilobytes</b> ] <b>rate packets</b> { <i>ppi</i>   <b>max</b> } <b>within</b> <i>seconds</i> [ <b>initial-delay</b> <i>packets</i> ] <b>no rate</b>
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>static-policer config>sys>security>dist-cpu-protection>policy>local-monitoring-policer config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters
<b>Description</b>	<p>This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.</p> <p>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, <b>show service id 33 sap 1/1/3:33 dist-cpu-protection detail</b>.</p>
<b>Default</b>	rate packets max within 1 initial delay 0
<b>Parameters</b>	<p><b>packets</b>   <b>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><i>ppi</i> — Specifies packets per interval. 0..255 or max (0 = all packets are nonconforming)</p> <ul style="list-style-type: none"> <li>• rate of max = effectively disable the policer (always conforming)</li> <li>• rate of packets 0 = all packets considered nonconforming.</li> </ul> <p><i>seconds</i> — Specifies the length of the ppi rate measurement interval.</p> <p><b>Values</b> 1 to 32767</p> <p><i>packets</i> — 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 to 255</p>

*kilobits-per-second* — Specifies the kilobits per second.

**Values** 1 to 20000000 | max max = This effectively disables the policer (always conforming).

**mbs** — The tolerance for the kbps rate

**Values** 0 to 4194304. A configured mbs of 0 will cause all packets to be considered nonconforming.

**Default** The default mbs sets the mbs to 10 ms of the kbps.

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

## protocol

**Syntax** [no] protocol *name* [create]

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

**Description** This command creates the protocol for control in the policy.

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 (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 (including RS/RA/Redirect) except NS/NA Neighbor Discovery packets which are 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 NS/NA Neighbor Discovery (not including RS/RA/Redirect which are classified as part of the protocol "icmp")
- ospf: includes all OSPFv2 and OSPFv3 packets.
- ppoe-pppoa: includes PADx, LCP, PAP/CHAP and NCPs

- **all-unspecified:** 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-unspecified” flow. The “all-unspecified” 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-unspecified protocol if the all-unspecified protocol is created in the policy.

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

## dynamic-parameters

<b>Syntax</b>	<b>dynamic-parameters</b>
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>protocol
<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).

## detection-time

<b>Syntax</b>	<b>detection-time</b> <i>seconds</i> <b>no detection-time</b>
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters
<b>Description</b>	When a dynamic enforcing policer is instantiated, it will remain allocated until at least a contiguous conforming period of detection-time passes.

## dynamic-enforcement-policer-pool

<b>Syntax</b>	<b>[no] dynamic-enforcement-policer-pool</b> <i>number-of-policers</i>
---------------	--



<b>Context</b>	config>card>fp>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>	no dynamic-enforcement-policer-pool
<b>Parameters</b>	<i>number-of-policers</i> — specifies the number of policers to be reserved.
<b>Values</b>	0, 1000 to 32000

## exceed-action

<b>Syntax</b>	<b>exceed-action</b> { <b>discard</b> [ <b>hold-down seconds</b> ]   <b>low-priority</b> [ <b>hold-down seconds</b> ]   <b>none</b> }
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters config>sys>security>dist-cpu-protection>policy>static-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>	exceed-action none
<b>Parameters</b>	<p><b>discard</b> — Discards packets that are nonconforming.</p> <p><b>low-priority</b> — Marks packets that are nonconforming as low-priority (for example, discard eligible or out-profile). If there is congestion in the control plane of the SR OS then unmarked (for example, green, hi-prio or in-profile) control packets are given preferential treatment.</p> <p><b>hold-down seconds</b> — When this optional parameter is specified, it causes the following “hold-down” behavior.</p> <p>When the 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.

Configuring the **indefinite** parameter value will cause hold down to remain 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.

Configuring the **none** parameter value will disable hold down.

**Values**      1 to 10080, indefinite, none

log-events

<b>Syntax</b>	<b>[no] log-events [verbose]</b> <b>no log-events</b>
<b>Context</b>	config>sys>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
<b>Parameters</b>	<b>verbose</b> — This parameter sends the send the same events as just “log-events” plus Hold Down Start, Hold Down End, DcpDynamicEnforceAlloc and DcpDynamicEnforceFreed events. This includes the allocation/de-allocation events (typically used for debug/tuning only – could be very noisy even when there is nothing much of concern).

enforcement

<b>Syntax</b>	<b>enforcement {static <i>policer-name</i>   dynamic {<i>mon-policer-name</i>   local-mon-bypass}}</b>
<b>Context</b>	config>sys>security>dist-cpu-protection>policy>protocol
<b>Description</b>	This command configures the enforcement method for the protocol.
<b>Default</b>	enforcement dynamic local-mon-bypass
<b>Parameters</b>	<b>static</b> — Specifies that 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.

*policer name* — Specifies the name is a static-policer.

**dynamic** — Specifies that 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 nonconforming state (at the end of a minimum monitoring time of 60 seconds to reduce thrashing).

*mon-policer-name* — Specifies which local-monitoring-policer to use

**local-mon-bypass** — 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.

## static-policer

<b>Syntax</b>	<b>[no] static-policer</b> <i>policer-name</i> <b>[create]</b>
<b>Context</b>	config>sys>security>dist-cpu-protection>policy
<b>Description</b>	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.
<b>Parameters</b>	<i>policy-name</i> — Specifies the name of the policy up to 32 characters in length.

## detection-time

<b>Syntax</b>	<b>detection-time</b> <i>seconds</i>
<b>Context</b>	config>sys>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 conforming 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>	detection-time 30
<b>Parameters</b>	<i>seconds</i> — Specifies the detection time.
<b>Values</b>	1 to 128000

---

## log-events

<b>Syntax</b>	<b>log-events [verbose]</b> <b>no log-events</b>
<b>Context</b>	config>sys>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>	log-events
<b>Parameters</b>	<b>verbose</b> — (Sends the same events as just “log-events” plus Hold Down Start and Down End events. The optional “verbose” includes some events that are more likely used during debug/tuning/investigations.

### 2.8.2.10 Extracted Protocol Traffic Priority Commands

## init-extract-prio-mode

<b>Syntax</b>	<b>init-extract-prio-mode {uniform   l3-classify}</b>
<b>Context</b>	config>card>fp
<b>Description</b>	This command determines the scheme used to select the initial drop priority of extracted control plane traffic. The initial drop priority of extracted packets can be either low or high priority. The drop priority of the extracted packets can be subsequently altered by mechanisms such as CPU protection. High-priority traffic receives preferential treatment in control plane congestion situations over low-priority traffic.
<b>Default</b>	init-extract-prio-mode uniform
<b>Parameters</b>	<p><b>uniform</b> — Initializes the drop priority of all extracted control traffic as high priority. Drop priority can then be altered (marked low priority) by distributed CPU protection (DCP) or centralized CPU protection rate-limiting functions in order to achieve protocol and interface isolation.</p> <p><b>l3-classify</b> — Initializes the drop priority of Layer 3 extracted control traffic (BGP and OSPF) based on the QoS classification of the packets. This is useful in networks where the DSCP and EXP markings can be trusted as the primary method to distinguish, protect, and isolate good terminating protocol traffic from unknown or potentially harmful protocol traffic instead of using the rate-based DCP and centralized CPU protection traffic marking/coloring mechanisms (for example, <b>out-profile-rate</b> and <b>exceed-action low-priority</b>).</p> <p>For network interfaces, the QoS classification profile result selects the drop priority (in = high priority, out = low priority) for extracted control traffic, and the default QoS classification maps different DSCP and EXP values to different in/out profile states.</p>

For access interfaces, the QoS classification priority result typically selects the drop priority for extracted control traffic. The default access QoS classification (**default-priority**) maps all traffic to **low**. If the queues in the access QoS policy are configured as **profile-mode** queues (rather than the default **priority-mode**) extracted traffic will use the QoS classification profile value configured against the associated FC (rather than the priority result) to select the drop priority.

Layer 2 extracted control traffic (ARP or ETH-CFM) and protocols that cannot always be QoS-classified, such as IS-IS, are initialized as low drop priority in order to protect Layer 2 protocol traffic on uniform interfaces (which would typically be subject to centralized CPU protection). Alternately, DCP can be used (by configuring a non-zero rate with **exceed-action** of **low-priority** for the **all-unspecified** protocol) to mark some of this traffic as high priority.

### 2.8.2.11 Security Password Commands

#### 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.

#### admin-password

<b>Syntax</b>	<b>admin-password</b> <i>password</i> [ <b>hash</b>   <b>hash2</b> ] <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</pre> <pre>&lt;global&gt; enable-admin</pre> <p>If the admin-password is configured in the <b>config&gt;system&gt;security&gt;password</b> 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>

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

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



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

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

For example:

```
file copy ftp://test:secret@10.20.31.79/test/srcfile cf1:\destfile
```

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

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

**Default** no admin-password

**Parameters**

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

**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.



**Note:** This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

aging

**Syntax**    **aging** *days*  
             **no aging**

---

<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>Parameters</b>	<p><i>days</i> — Specifies the maximum number of days the password is valid.</p> <p><b>Values</b> 1 to 500</p>



**Note:** This command applies to local users.

## attempts

<b>Syntax</b>	<p><b>attempts</b> <i>count</i> [<b>time</b> <i>minutes1</i> [<b>lockout</b> <i>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>	attempts 3 time 5 lockout 10
<b>Parameters</b>	<p><i>count</i> — Specifies 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 to 64</p> <p><i>minutes</i> — Specifies 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 to 60</p> <p><i>minutes</i> — Specifies the lockout period, in minutes, during which the user is not allowed to login.</p> <p><b>Values</b> 0 to 1440, or infinite</p>

If 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 lockout time period.

**Values** 0 to 1440

**Values** infinite; user is locked out and must wait until manually unlocked before any further attempts.



**Note:** This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

enable-admin

<b>Syntax</b>	<b>enable-admin</b>
<b>Context</b>	<global>
<b>Description</b>	Refer to the description for the <a href="#">admin-password</a> command. If the <b>admin-password</b> is configured in the <b>config&gt;system&gt;security&gt;password</b> context, then any user can enter the special administrative mode by entering the command.

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

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

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

To verify that a user is in the enable-admin mode, perform one of the following steps:

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

```
*A:node-1# show users
=====
User                               Type      Login time      Idle time
  Session ID   From
=====
                               Console      --              3d 10:16:12 --
6
admin                               SSHv2      12OCT2018 20:44:15  0d 00:00:00 A-
#83                               192.168.255.255
admin                               SSHv2      12OCT2018 21:09:25  0d 00:05:10 --
84                               192.168.255.255
-----
Number of users: 2
'#' indicates the current active session
'A' indicates user is in admin mode
=====
```



```
*A:node-1# enable-admin
MINOR: CLI Already in admin mode.
*A:node-1#
```

## authentication-order

<b>Syntax</b>	<b>authentication-order</b> [ <i>method-1</i> ] [ <i>method-2</i> ] [ <i>method-3</i> ] [ <i>method-4</i> ] [ <b>exit-on-reject</b> ] <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 local passwords, RADIUS, TACACS+, and LDAP.</p> <p>The authentication 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 documents the failed attempt. Both the attempted login identification and originating IP address are 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>	authentication-order radius tacplus ldap local - The preferred order for password authentication is 1. local passwords, 2. RADIUS, 3. TACACS+, and 4. LDAP.
<b>Parameters</b>	<p><i>method-1</i> — Specifies the first password authentication method to attempt.</p> <p><b>Values</b> local, radius, tacplus, ldap</p> <p><i>method-2</i> — Specifies the second password authentication method to attempt.</p> <p><b>Values</b> local, radius, tacplus, ldap</p> <p><i>method-3</i> — Specifies the third password authentication method to attempt.</p> <p><b>Values</b> local, radius, tacplus, ldap</p> <p><i>method-4</i> — Specifies the fourth password authentication method to attempt.</p> <p><b>Values</b> local, radius, tacplus, ldap</p> <p><b>local</b> — Specifies the password authentication based on the local password database.</p> <p><b>radius</b> — Specifies RADIUS authentication.</p> <p><b>tacplus</b> — Specifies TACACS+ authentication.</p> <p><b>ldap</b> — Specifies LDAP authentication.</p>

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

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

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



**Note:** This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

complexity-rules

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



**Note:** This command applies to local users.

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.  The <b>no</b> form of the command does not allow user name to be used as password.
<b>Default</b>	no allow-user-name

## credits

<b>Syntax</b>	<b>credits</b> [ <b>lowercase</b> <i>credits</i> ] [ <b>uppercase</b> <i>credits</i> ] [ <b>numeric</b> <i>credits</i> ] [ <b>special-character</b> <i>credits</i> ] <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.  The <b>no</b> form of the command resets to default.
<b>Default</b>	no credits
<b>Parameters</b>	<i>credits</i> — Specifies the number of credits that can be used for each characters class. <b>Values</b> 0 to 10

## minimum-classes

<b>Syntax</b>	<b>minimum-classes</b> <i>minimum</i> <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  The <b>no</b> form of the command resets to default.
<b>Default</b>	no minimum-classes
<b>Parameters</b>	<i>minimum</i> — Specifies the minimum number of classes to be configured. <b>Values</b> 2 to 4

## minimum-length

<b>Syntax</b>	<b>minimum-length</b> <i>length</i> <b>no minimum-length</b>
<b>Context</b>	config>system>security>password>complexity-rules
<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.  If multiple minimum-length commands are entered each command overwrites the previous entered command.

---

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

<b>Default</b>	minimum-length 6
<b>Parameters</b>	<i>value</i> — Specifies the minimum number of characters required for a password.
<b>Values</b>	1 to 8

## repeated-characters

<b>Syntax</b>	<b>repeated-characters</b> <i>count</i> <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.  The <b>no</b> form of the command resets to default.
<b>Default</b>	no repeated-characters
<b>Parameters</b>	<i>count</i> — Specifies the minimum count of consecutively repeated characters. <b>Values</b> 2 to 8

## required

<b>Syntax</b>	<b>required</b> [ <b>lowercase</b> <i>count</i> ] [ <b>uppercase</b> <i>count</i> ] [ <b>numeric</b> <i>count</i> ] [ <b>special-character</b> <i>count</i> ] <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.  The <b>no</b> form of the command resets to default.
<b>Default</b>	required lowercase 0 uppercase 0 numeric 0 special-character 0
<b>Parameters</b>	<i>count</i> — Specifies the minimum count of characters classes. <b>Values</b> 0 to 10

## dynsvc-password

<b>Syntax</b>	<b>dynsvc-password</b> <i>password</i> [ <b>hash</b>   <b>hash2</b> ] <b>no dynsvc-password</b>
<b>Context</b>	config>system>security>password

<b>Description</b>	This command configures the password which enables the user to configure dynamic services.
<b>Default</b>	no dynsvc-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> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the <b>hash2</b> encrypted variable cannot be copied and pasted. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified.</p>



**Note:** This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

## 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.



**Note:** This command applies to users on RADIUS, TACACS, and LDAP.

## tacplus-map-to-priv-lvl

<b>Syntax</b>	<b>tacplus-map-to-priv-lvl</b> [ <i>admin-priv-lvl</i> ] <b>no tacplus-map-to-priv-lvl</b>
<b>Context</b>	config>system>security>password>enable-admin-control

**Description** When **tacplus-map-to-priv-lvl** is enabled, and tacplus authorization is enabled with the *use-priv-lvl* option, typing **enable-admin** starts an interactive authentication exchange from the 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 **config>system>security>tacplus>priv-lvl-map**).

## health-check

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

**Context** config>system>security>password

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

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

**Default** health-check interval 30

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

<b>Values</b>	6 to 1500
<b>Default</b>	30

## history-size

**Syntax** **history-size size**  
**no history-size**

**Context** config>system>security>password

**Description** Configure how many previous passwords a new password is matched against.

**Default** no history

**Parameters** *size* — Specifies how many previous passwords a new password is matched against.

<b>Values</b>	0 to 20
<b>Default</b>	0

## minimum-age

<b>Syntax</b>	<b>minimum-age</b> [ <b>days</b> <i>days</i> ] [ <b>hrs</b> <i>hours</i> ] [ <b>min</b> <i>minutes</i> ] [ <b>sec</b> <i>seconds</i> ] <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>	minimum-age min 10
<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 to 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 to 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 to 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 to 59</p>



**Note:** This command applies to local users.

## minimum-change

<b>Syntax</b>	<b>minimum-change</b> <i>distance</i> <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>	minimum-change 5

---

<b>Parameters</b>	<i>distance</i> — Specifies how many characters must be different in the new password from the old password.
<b>Values</b>	1 to 20



**Note:** This command applies to local users.

### 2.8.2.12 Public Key Infrastructure (PKI) Commands

The commands described in the following section apply to the 7450 ESS and 7750 SR.

#### 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> [create] <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 cannot be removed until all the associations (ipsec-tunnel/gw) have been removed.</p>
<b>Parameters</b>	<i>name</i> — Specifies the name of the <b>ca-profile</b> , a string up to 32 characters.



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

## cert-file

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

### Notes:

- The system will perform following checks against configured cert-file when a **no shutdown** command is issued:
  - Configured cert-file must be a DER formatted X.509v3 certificate file.
  - All non-optional fields defined in section 4.1 of RFC5280 must exist and conform to the 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.

## cmpv2

**Syntax** **cmpv2**

---

<b>Context</b>	config>system>security>pki>ca-profile
<b>Description</b>	This command enables the context to configure Certificate Management Protocol Version 2 (CMPv2) parameters.

## 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>	<p>This command enables the system to accept both protected and unprotected CMPv2 error message. Without this command, system will only accept protected error messages.</p> <p>The <b>no</b> form of the command causes the system to only accept protected PKI confirmation message.</p>
<b>Default</b>	no accept-unprotected-errormsg

## 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>	<p>This command enables the system to accept both protected and unprotected CMPv2 PKI confirmation messages. Without this command, the system will only accept protected PKI confirmation message.</p> <p>The <b>no</b> form of the command causes the system to only accept protected PKI confirmation message.</p>
<b>Default</b>	no accept-unprotected-pkiconf

## http-response-timeout

<b>Syntax</b>	<b>http-response-timeout</b> <i>timeout</i> <b>no http-response-timeout</b>
<b>Context</b>	config>system>security>pki>ca-profile>cmpv2
<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>	http-response-timeout 30

---

**Parameters**    *timeout* — Specifies the HTTP response timeout in seconds.  
**Values**        1 to 3600

## key-list

**Syntax**        **key-list**  
**Context**       config>system>security>pki>ca-profile>cmpv2  
**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>cmpv2>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 the SR OS hash2 algorithm.  
The **no** form of the command removes the parameters from the configuration.  
**Parameters**    *password* — Specifies a printable ASCII string, up to 64 characters in length.  
**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified  
**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.  
*reference-number* — Specifies a printable ASCII string, up to 64 characters in length.

## response-signing-cert

**Syntax**        **response-signing-cert** *filename*  
**no response-signing-cert**


---

<b>Context</b>	config>system>security>pki>ca-profile>cmp2
<b>Description</b>	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.
<b>Default</b>	no response-signing-cert
<b>Parameters</b>	<i>filename</i> — Specifies the filename of the imported certificate.

## same-recipnonce-for-pollreq

<b>Syntax</b>	[no] same-recipnonce-for-pollreq
<b>Context</b>	config>system>security>pki>ca-profile>cmp2
<b>Description</b>	<p>This command enables the system to use same recipNonce as the last CMPv2 response for poll request.</p> <p>The <b>no</b> form of the command disables system to use same recipNonce as the last CMPv2 response for poll request.</p>
<b>Default</b>	no same-recipnonce-for-pollreq

## url

<b>Syntax</b>	<b>url</b> <i>url-string</i> [ <b>service-id</b> <i>service-id</i> ] <b>url</b> <i>url-string</i> [ <b>service-name</b> <i>service-name</i> ] <b>no url</b>
<b>Context</b>	config>system>security>pki>ca-profile>cmp2
<b>Description</b>	<p>This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles.</p> <p>The URL will be resolved by the DNS server configured (if configured) in the corresponding router context.</p> <p>If the <i>service-id</i> 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.</p>
	<div> <b>Note:</b> If the service is VPRN, then the system only allows HTTP ports 80 and 8080.</div>
<b>Parameters</b>	<i>url-string</i> — Specifies the HTTP URL of the CMPv2 server up to 180 characters in length.

**service-id** *service-id* — Specifies the service instance that used to reach CMPv2 server.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The *url-string* **service-name** *service-name* variant can be used in all configuration modes.

**Values**      service-id: 1 to 2147483647  
                 base-router: 0

**service-name** *service-name* — Identifies the service, up to 64 characters.

## crl-file

<b>Syntax</b>	<b>crl-file</b> <i>filename</i> <b>no crl-file</b>
<b>Context</b>	config>system>security>pki>ca-profile
<b>Description</b>	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> .

Notes:

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

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

<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

---

**Description** This command enables the context to configure OCSP parameters.

## responder-url

**Syntax** **responder-url** *url-string*  
**no responder-url**

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

**Description** 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.

**Default** no responder-url

**Parameters** *url-string* — Specifies the HTTP URL of the OCSP responder

## service

**Syntax** **service** *service-id*  
**service name** *service-name*  
**no service**

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

**Description** 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.

The responder-url will also be resolved by using the DNS server configured in the configured routing instance.

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.

**Parameters** *service-id* — Specifies an existing service ID to be used in the match criteria.  
This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **service name** *service-name* variant can be used in all configuration modes.

**Values** service-id: 1 to 2147483647  
base-router: 0

**name** *service-name* — Identifies the service, up to 64 characters.

## certificate-display-format

<b>Syntax</b>	<b>certificate-display-format</b> { <b>ascii</b>   <b>utf8</b> }
<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>	certificate-display-format ascii
<b>Parameters</b>	<p><b>ascii</b> — Specifies the ASCII format to use for the Certificates and Certificate Revocation Lists.</p> <p><b>utf8</b> — Specifies the UTF8 format to use for the Certificates and Certificate Revocation Lists.</p>

## certificate-expiration-warning

<b>Syntax</b>	<b>certificate-expiration-warning</b> <i>hours</i> [ <b>repeat</b> <i>repeat-hours</i> ] <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>

This command specifies when system will issue **BeforeExp** message before a certificate expires. For example, with **certificate-expiration-warning 5**, the system will issue a **BeforeExp** message 5 hours before a certificate expires. An optional **repeat** *<repeat-hour>* parameter will enable the system to repeat the **BeforeExp** message every hour until the certificate expires.

If the user only wants **AfterExp**, then **certificate-expiration-warning 0** can be used to achieve this.

**BeforeExp** and **AfterExp** warnings can be cleared in following cases:

- The certificate is reloaded by the **admin certificate reload** command. In this case, if the reloaded file is not expired, then **AfterExp** is cleared. And, if the reloaded file is outside of configured warning window, then the **BeforeExp** is also cleared.
- When the **ca-profile/ipsec-gw/ipsec-tunnel/cert-profile** is shutdown, then **BeforeExp** and **AfterExp** of corresponding certificates are cleared.
- When **no certificate-expiration-warning** command is configured, then all existing **BeforeExp** and **AfterExp** are cleared.

- Users may change the configuration of the **certificate-expiration-warning** so that certain certificates are no longer in the warning window. **BeforeExp** of corresponding certificates are cleared.
- If the system time changes so that the new time causes the certificates to no longer be in the warning window, then **BeforeExp** is cleared. If the new time causes an expired certificate to come non-expired, then **AfterExp** is cleared.

<b>Default</b>	no certificate-expiration-warning
<b>Parameters</b>	<p><i>hours</i> — Specifies the amount of time before a certificate expires when system issues BeforeExp.</p> <p><b>Values</b> 0 to 8760</p> <p><i>repeat-hours</i> — Specifies the time the system will repeat BeforeExp every repeat-hour.</p> <p><b>Values</b> 0 to 8760</p>

## common-name-list

<b>Syntax</b>	<b>common-name-list</b> <i>name</i> [ <b>create</b> ]
<b>Context</b>	config>system>security>pki
<b>Description</b>	This command configures a list of common names (CNs) that will be used to authenticate X.509.3 certificates. If the CN field of the X.509.3 certificate matches any of the CNs in the list, then the certificate can be used.
<b>Parameters</b>	<i>name</i> — Specifies the name of the CN list, up to 32 characters maximum.

## cn

<b>Syntax</b>	[ <b>no</b> ] <b>cn</b> <i>index type type value common-name-value</i>
<b>Context</b>	config>system>security>pki>common-name-list
<b>Description</b>	<p>This command creates a CN list entry in text or regexp format.</p> <p>The <b>no</b> form of the command removes the specified entry.</p>
<b>Parameters</b>	<p><i>index</i> — Specifies the index number of the entry.</p> <p><i>type</i> — Specifies the type of the entry.</p> <p><b>Values</b> ip-address, domain-name</p> <p><i>common-name-value</i> — Specifies the IP address or domain name value, up to 255 characters maximum.</p>



## crl-expiration-warning

<b>Syntax</b>	<b>crl-expiration-warning</b> <i>hours</i> [ <b>repeat</b> <i>repeat-hours</i> ] <b>no</b> <b>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> <i>&lt;repeat-hour&gt;</i> 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</b> <b>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 to 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 to 8760</p>

## maximum-cert-chain-depth

<b>Syntax</b>	<b>maximum-cert-chain-depth</b> <i>level</i> <b>no</b> <b>maximum-cert-chain-depth</b>
<b>Context</b>	config>system>security>pki
<b>Description</b>	This command defines the maximum depth of certificate chain verification. This number is applied system wide.

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

<b>Default</b>	maximum-cert-chain-depth 7
<b>Parameters</b>	<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.
<b>Values</b>	1 to 7

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>security>pki>ca-profile>
<b>Description</b>	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.  The ca-profile in a <b>shutdown</b> state cannot be used in certificate authentication.
<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. For information about CMPv6 admin certificate commands, see the <i>7450 ESS</i> , <i>7750 SR</i> , and <i>VSR Multiservice Integrated Service Adapter Guide</i> .

## 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>	<i>entry-id</i> — Specifies the local cache entry identifier of the certificate to clear.
<b>Values</b>	1 to 2000

## crl-update

<b>Syntax</b>	<b>crl-update ca</b> <i>ca-profile-name</i>
<b>Context</b>	admin>certificate
<b>Description</b>	<p>This command manually triggers the Certificate Revocation List file (CRL) update for the specified ca-profile.</p> <p>Using this command requires shutting down the auto-crl-update.</p>
<b>Parameters</b>	<i>ca-profile-name</i> — Specifies the name of the Certificate Authority profile.

## display

<b>Syntax</b>	<b>display type</b> { <i>type</i> } <i>url-string</i> <b>format</b> { <i>format</i> } [ <b>password</b> [32 chars max]]
<b>Context</b>	admin>certificate
<b>Description</b>	This command displays the content of an input file in plain text.



**Note:** When displaying the key file content, only the key size and type are displayed.

The following list summarizes the formats supported by this command:

- System
  - 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

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

**Values**

url-string	<local-url> - [99 chars max]
local-url	<cf-flash-id>/<file-path>
cf-flash-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 an encrypted PKCS#12 file, up to 99 characters in length.

## export

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

**Context** admin>certificate

**Description** This command performs certificate operations.

## gen-keypair

**Syntax** **gen-keypair url-string curve** {**secp256r1** | **secp384r1** | **secp521r1**}  
**gen-keypair url-string** [**size** {**512** | **1024** | **2048**}] [**type** {**rsa** | **dsa**}]

**Context** admin>certificate

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

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

**Values**

url-string	<local-url> - [99 chars max]
local-url	<cf-flash-id>/<file-path>
cf-flash-id	cf1:   cf2:   cf3:

**curve** — Generates an ECDSA key with a specified curve.

**Values** secp256r1, secp384r1, secp521r1

**size** — Specifies the key size in bits.

The minimum key-size is 1024 when running in FIPS-140-2 mode.

**Values** 512, 1024, 2048

**Default** 2048

**type** — Specifies the type of key.

**Values** rsa, dsa

**Default** rsa

## gen-local-cert-req

**Syntax** **gen-local-cert-req** **keypair** *url-string* **subject-dn** *subject-dn* [**domain-name** *name*] [**ip-addr** *ip-address*] **file** *url-string* [**hash-alg** *hash-algorithm*]

**Context** admin>certificate

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

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

**Values**

url-string	<local-url> - [99 chars max]
local-url	<cf-flash-id>/<file-path>
cf-flash-id	cf1:   cf2:   cf3:

**subject-dn** — 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* — Specifies a domain name string can be specified and included as the dNSName in the Subject Alternative Name extension of the certificate request.

*ip-address* — Specifies 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* — Specifies the certificate 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-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   crt} 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><li>– PKCS #7 DER encoded</li><li>– PEM</li><li>– DER</li></ul></li></ul>



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

<b>Default</b>	none
<b>Parameters</b>	<p><b>input url-string</b> — 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.</p> <p><b>output url-string</b> — Specifies the name of output file up to 95 characters in length. The output directory depends on the file type like following:</p>

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

**Values**

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

**type** — The type of input file.

**Values** cert, key, crl

**format** — Specifies the format of input file.

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

**password** — Specifies the password to decrypt the input file in case that it is an 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-tunnel/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 exists or somehow invalid (bad format, does not contain right extension, and so on), 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** — Specifies the key filename. IF the cert-key-pair is enabled, the filename is the imported filename of certificate, *key-filename* is the imported key file.

secure-nd-export

<b>Syntax</b>	<b>secure-nd-export</b>
<b>Context</b>	admin>certificate
<b>Description</b>	This command exports IPv6 Secure Neighbor Discovery (SeND) certificates to the file cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.

secure-nd-import

<b>Syntax</b>	<b>secure-nd-import</b> <i>url-string</i> <b>format</b> <i>input-format</i> [ <b>password</b> <i>password</i> ] [ <b>key-rollover</b> ]		
<b>Context</b>	admin>certificate		
<b>Description</b>	This command imports IPv6 Secure Neighbor Discovery (SeND) certificates from a file, and saves them to cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.		
<b>Parameters</b>	<i>url-string</i> — Specifies the name of an input file up to 99 characters in length.		
	<b>Values</b>	local-url	<cf-flash-id>\<file-path>
		cf-flash-id	cf1: cf2: cf3:
	<i>input-format</i> — Specifies the input file format.		
	<b>Values</b>	pkcs12, pem, or der	
	<i>password</i> — Specifies the password to decrypt the input file if it is an encrypted PKCS#12 file.		
	<b>Values</b>	32 characters maximum	



### 2.8.2.13 Profile Commands

#### 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 <a href="#">user</a> 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>	profile default
<b>Parameters</b>	<i>user-profile-name</i> — Specifies the user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

#### default-action

<b>Syntax</b>	<b>default-action</b> { <b>deny-all</b>   <b>permit-all</b>   <b>none</b>   <b>read-only-all</b> }
<b>Context</b>	config>system>security>profile
<b>Description</b>	This command specifies the default action to be applied when no match conditions are met.
<b>Parameters</b>	<b>deny-all</b> — Sets the default of the profile to deny access to all commands. <b>permit-all</b> — Sets the default of the profile to permit access to all commands.



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

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

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

## entry

<b>Syntax</b>	<b>[no] entry</b> <i>entry-id</i>
<b>Context</b>	config>system>security>profile
<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>Parameters</b>	<p><i>entry-id</i> — Specifies an entry-id that 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 to 9999</p>

## action

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

## match

<b>Syntax</b>	<b>match</b> <i>command-string</i> <b>no match</b>
<b>Context</b>	config>system>security>profile>entry
<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>Parameters</b>	<i>command-string</i> — Specifies the CLI command or CLI tree level that is the scope of the profile entry.

## grpc

<b>Syntax</b>	<b>grpc</b>
<b>Context</b>	config>system>security>profile
<b>Description</b>	This command enables the context to configure a specific gRPC security profile.

## rpc-authorization

<b>Syntax</b>	<b>rpc-authorization</b>
<b>Context</b>	config>system>security>profile>grpc
<b>Description</b>	This command opens a configuration context for configuring user privileges related to RPCs.

## gnmi-capabilities

<b>Syntax</b>	<b>gnmi-capabilities</b> {deny   permit}
<b>Context</b>	config>system>security>profile>grpc>rpc-authorization
<b>Description</b>	This command permits or denies use of Capability RPC for a user associated with the given format.
<b>Default</b>	gnmi-capabilities permit

---

**Parameters**     **deny** — Denies use of Capability RPC.  
                     **permit** — Permits use of Capability RPC.

## gnmi-get

**Syntax**     **gnmi-get {deny | permit}**

**Context**     config>system>security>profile>grpc>rpc-authorization

**Description**     This command permits or denies the Get RPC.

**Default**     gnmi-get permit

**Parameters**     **deny** — Denies use of Get RPC.  
                     **permit** — Permits use of Get RPC.

## gnmi-set

**Syntax**     **gnmi-set {deny | permit}**

**Context**     config>system>security>profile>grpc>rpc-authorization

**Description**     This command permits or denies the Set RPC.

**Default**     gnmi-set permit

**Parameters**     **deny** — Denies use of Set RPC.  
                     **permit** — Permits use of Set RPC.

## gnmi-subscribe

**Syntax**     **gnmi-subscribe {deny | permit}**

**Context**     config>system>security>profile>grpc>rpc-authorization

**Description**     This command permits or denies the Subscribe RPC.

**Default**     gnmi-subscribe permit

**Parameters**     **deny** — Denies use of Subscribe RPC.  
                     **permit** — Permits use of Subscribe RPC.

## rib-api-getversion

<b>Syntax</b>	<b>rib-api-getversion {deny   permit}</b>
<b>Context</b>	config>system>security>profile>grpc>rpc-authorization
<b>Description</b>	This command permits or denies the use of the GetVersion RPC provided by the RibApi service.
<b>Default</b>	rib-api-getversion permit
<b>Parameters</b>	<b>deny</b> — Denies use of GetVersion RPC. <b>permit</b> — Permits use of GetVersion RPC.

## rib-api-modify

<b>Syntax</b>	<b>rib-api-modify {deny   permit}</b>
<b>Context</b>	config>system>security>profile>grpc>rpc-authorization
<b>Description</b>	This command permits or denies the use of the Modify RPC provided by the RibApi service.
<b>Default</b>	rib-api-modify permit
<b>Parameters</b>	<b>deny</b> — Denies use of Modify RPC. <b>permit</b> — Permits use of Modify RPC.

## li

<b>Syntax</b>	<b>[no] li</b>
<b>Context</b>	config>system>security>profile
<b>Description</b>	This command enables the Lawful Intercept (LI) profile identifier. The <b>no</b> form of the command disables the LI profile identifier.

## renum

<b>Syntax</b>	<b>renum <i>old-entry-number new-entry-number</i></b>
<b>Context</b>	config>system>security>profile
<b>Description</b>	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 to 9999

*new-entry-number* — Enter the new entry number.

**Values** 1 to 9999

### 2.8.2.14 CLI Session Commands

## cli-session-group

**Syntax** `cli-session-group session-group-name [create]`  
`no cli-session-group session-group-name`

**Context** config>system>security

<b>Description</b>	This command is used to configure a session group that can be used to limit the number of CLI sessions available to members of the group.
--------------------	---

**Parameters** *session-group-name* — Specifies a particular session group.

## combined-max-sessions

**Syntax**    **combined-max-sessions** *number-of-sessions*  
**no combined-max-sessions**

**Context** config>system>security>cli-session-group  
config>system>security>profile

<b>Description</b>	This command is used to limit the number of combined SSH/TELENT based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.
--------------------	---

The **no** form of this command disables the command and the profile/group limit is not applied to the number of combined sessions.

**Default** no combined-max-sessions

**Parameters**    *number-of-sessions* — Specifies the maximum number of allowed combined SSH/TELNET based CLI sessions.

**Values** 0 to 50

---

## ssh-max-sessions

<b>Syntax</b>	<b>ssh-max-sessions</b> <i>number-of-sessions</i> <b>no ssh-max-sessions</b>
<b>Context</b>	config>system>security>cli-session-group config>system>security>profile
<b>Description</b>	<p>This command is used to limit the number of SSH-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.</p> <p>The <b>no</b> form of this command disables the command and the profile/group limit is not applied on the number of sessions.</p>
<b>Default</b>	no ssh-max-sessions
<b>Parameters</b>	<i>number-of-sessions</i> — Specifies the maximum number of allowed SSH-based CLI sessions. <b>Values</b> 0 to 50

## telnet-max-sessions

<b>Syntax</b>	<b>telnet-max-sessions</b> <i>number-of-sessions</i> <b>no telnet-max-sessions</b>
<b>Context</b>	config>system>security>cli-session-group config>system>security>profile
<b>Description</b>	<p>This command is used to limit the number of Telnet-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.</p> <p>The <b>no</b> form of this command disables the command and the profile/group limit is not applied on the number of sessions.</p>
<b>Default</b>	no telnet-max-sessions
<b>Parameters</b>	<i>number-of-sessions</i> — Specifies the maximum number of allowed Telnet-based CLI sessions. <b>Values</b> 0 to 50

---

## 2.8.2.15 RADIUS Commands

### 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.  Implement redundancy by configuring multiple server addresses for each router.  The <b>no</b> form of the command removes the RADIUS configuration.

### access-algorithm

<b>Syntax</b>	<b>access-algorithm {direct   round-robin}</b> <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>	access-algorithm direct
<b>Parameters</b>	<b>direct</b> — The first server will be used as primary server for all requests, the second as secondary and so on.  <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.

### accounting

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



---

## accounting-port

<b>Syntax</b>	<b>accounting-port</b> <i>port</i> <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>Default</b>	accounting-port 1813				
<b>Parameters</b>	<i>port</i> — Specifies the UDP port number. <table><tr><td><b>Values</b></td><td>1 to 65535</td></tr><tr><td><b>Default</b></td><td>1813</td></tr></table>	<b>Values</b>	1 to 65535	<b>Default</b>	1813
<b>Values</b>	1 to 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] interactive-authentication</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 interactive-authentication

## port

<b>Syntax</b>	<b>port</b> <i>port</i> <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.

---

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

<b>Default</b>	port 1812 (as specified in RFC 2865, <i>Remote Authentication Dial In User Service (RADIUS)</i> )
<b>Parameters</b>	<i>port</i> — Specifies the TCP port number to contact the RADIUS server.
<b>Values</b>	1 to 65535

## retry

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

## server

<b>Syntax</b>	<b>server</b> <i>index</i> <b>address</b> <i>ip-address</i> <b>secret</b> <i>key</i> [ <b>hash</b>   <b>hash2</b> ] <b>no</b> <b>server</b> <i>index</i>
<b>Context</b>	config>system>security>radius
<b>Description</b>	This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.  Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.  The <b>no</b> form of the command removes the server from the configuration.
<b>Default</b>	no server

**Parameters**     *index* — Specifies the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

**Values**            1 to 5

*ip-address* — Specifies the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

**Values**

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

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

**Values**            Up to 64 characters in length.

**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

## timeout

<b>Syntax</b>	<b>timeout</b> <i>seconds</i> <b>no timeout</b>
<b>Context</b>	config>system>security>radius
<b>Description</b>	This command configures the number of seconds the router waits for a response from a RADIUS server.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	timeout 3

---

<b>Parameters</b>	<i>seconds</i> — Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.
<b>Values</b>	1 to 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 default 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_default user-template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server and radius authorization is enabled.</p> <p>The no form of the command disables the use of the RADIUS default template.</p>
<b>Default</b>	no use-default-template

### 2.8.2.16 TACACS+ Client Commands

## 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> <b>no accounting</b>
<b>Context</b>	config>system>security>tacplus
<b>Description</b>	<p>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.</p>

---

<b>Default</b>	no accounting
<b>Parameters</b>	<p><b>record-type start-stop</b> — Specifies that a TACACS+ start packet is sent whenever the user executes a command and a TACACS+ stop packet when command execution is complete.</p> <p><b>record-type stop-only</b> — Specifies that only a TACACS+ 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
<b>Parameters</b>	<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 the 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>• The 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>• The SR OS displays the <i>server_msg</i>, and collects the user name.</li> <li>• The 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>• The 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> </ul>

- The SR OS sends a continue message with the password.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is disabled the 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 (while this is non-standard, it does not cause interoperability problems).
- TACACS+ server ignores the password and replies with TAC\_PLUS\_AUTHEN\_STATUS\_GETPASS.
- The 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

## priv-lvl-map

**Syntax** [no] **priv-lvl-map**

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

**Description** This command enables the context 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.

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

**Default** priv-lvl-map

## priv-lvl

**Syntax** **priv-lvl** *priv-lvl user-profile-name*  
**no priv-lvl** *priv-lvl*

**Context** config>system>security>tacplus>priv-lvl-map

**Description** This command maps a specific TACACS+ priv-lvl to a locally configured profile for authorization. This mapping is used when the **use-priv-lvl** option is specified for TACPLUS authorization.

**Parameters** *priv-lvl* — Specifies the privilege level used when sending a TACACS+ ENABLE request.  
**Values** 0 to 15  
*user-profile-name* — Specifies the user profile for this mapping.

## server

**Syntax** **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2**][**port** *port*]  
**no server** *index*

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

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

Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.

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

**Default** No TACACS+ servers are configured.

**Parameters** *index* — Specifies the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.  
**Values** 1 to 5

*ip-address* — Specifies the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.  
**Values**

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

**secret** *key* — Specifies the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.  
**Values** Up to 128 characters in length.

**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

**port** — Specifies the port ID.

**Values** 0 to 65535

## 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

## timeout

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

## use-default-template

<b>Syntax</b>	<b>[no] use-default-template</b>
---------------	----------------------------------



---

<b>Context</b>	config>system>security>tacplus
<b>Description</b>	This command specifies whether the tacplus_default user-template is actively applied to the TACACS+ user. When enabled, the tacplus_default user-template is actively applied if tacplus authorization is enabled (without the use-priv-lvl option).
<b>Default</b>	use-default-template

## 2.8.2.17 LDAP Client Commands

### ldap

<b>Syntax</b>	[no] ldap
<b>Context</b>	config>system>security
<b>Description</b>	This command configures LDAP authentication parameters for the system.  The <b>no</b> form will de-configure the LDAP client from the SR OS.

### public-key-authentication

<b>Syntax</b>	[no] public-key-authentication
<b>Context</b>	config>system>security>ldap
<b>Description</b>	This command enables public key retrieval from the LDAP server. If disabled (in its <b>no</b> form), password authentication will be attempted via LDAP.
<b>Default</b>	no public-key-authentication

### retry

<b>Syntax</b>	<b>retry</b> <i>count</i> <b>no</b> <b>retry</b>
<b>Context</b>	config>system>security>ldap
<b>Description</b>	This command configures the number of retries for the SR OS in its attempt to reach the current LDAP server before attempting the next server.  The <b>no</b> version of this command will revert to the default value.
<b>Default</b>	retry 3

**Parameters**     *count* — Specifies the number of retransmissions.

**Values**     1 to 10

**Default**    3

server

**Syntax**     **server** *server-index* [**create**]  
                  **no server** *server-index*

**Context**     config>system>security>ldap

**Description**     This command configures an LDAP server. Up to five servers can be configured, which can then work in a redundant manner.

                  The **no** version of this command removes the server connection.

**Parameters**     *server-index* — Specifies a unique LDAP server connection.

**Values**     1 to 5

address

**Syntax**     **address** *ip-address* [**port** *port*]  
                  **no address**

**Context**     config>system>security>ldap>server

**Description**     This command configures the IPv4 or IPv6 address for the LDAP server.

                  The **no** version of this command removes the server address.

**Parameters**     *ip-address* — The IP address of the LDAP server.

**Values**

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

*port* — Specifies the port ID. The port is the LDAP server listening port; by default it is 389 but if the listening port on LDAP server is changed, this command needs to be configured accordingly.

**Values**     1 to 65535

**Default**    389

## bind-authentication

- Syntax** **bind-authentication** *root-dn* [**password** *password*] [**hash** | **hash2**]  
**no bind-authentication**
- Context** config>system>security>ldap>server
- Description** This command configures the LDAP binding used to log into LDAP server. A string of domain components (DC) and common names (CN) can be programmed to identify the user in addition to the password field. The password is hashed. For example, "cn=admin,dc=nokia,dc=com" indicates the user admin in domain nokia.com. [Table 31](#) lists the LDAP attributes.

The **no** version of this command removes the bind-authentication.

**Table 31 LDAP Attributes**

Object Class	Naming Attribute Display Name	Naming Attribute LDAP Name
user	Common-Name	cn
organizationalUnit	Organizational-Unit-Name	ou
domain	Domain-Component	dc

- Parameters** *root-dn* — Up to 512 characters.
- password* — Configures the password which enables a user to bind to the LDAP server. The maximum length is 128 characters.
- hash** — Specifies that the password is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the password is assumed to be in an unencrypted, clear text form. For security, all passwords are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified
- hash2** — Specifies the password is entered in a more complex encrypted form that involves more variables than the password value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the password is assumed to be in an unencrypted, clear text form. For security, all passwords are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

## ldap-server

- Syntax** **ldap-server** *server-name*  
**no ldap-server**
- Context** config>system>security>ldap>server

---

<b>Description</b>	This command configures the LDAP server name or description.  The <b>no</b> version of this command removes the LDAP server name.
<b>Parameters</b>	<i>server-name</i> — Specifies the name of the server, up to 32 characters.

## search

<b>Syntax</b>	<b>search</b> <i>base-dn</i> <b>no search</b>
<b>Context</b>	config>system>security>ldap>server
<b>Description</b>	This command configures the LDAP <b>search</b> command. The search <i>base-dn</i> tells the server which part of the external directory tree to search. The search DN uses the same LDAP attribute as <i>root-dn</i> . For example, to search a public-key for an SSH generated for a Nokia vendor, one might use “dc=public-key,dc=nokia,dc=com”.  The <b>no</b> version of this command remove the search DN; as such, no search will be possible on the LDAP server.
<b>Parameters</b>	<i>base-dn</i> — Specifies the base domain name used in the search, up to 512 characters.

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>security>ldap config>system>security>ldap>server
<b>Description</b>	In the <b>ldap</b> context, this command enables or disabled LDAP protocol operations.  In the <b>server</b> context, this command enables or disables the LDAP server. To perform <b>no shutdown</b> , an LDAP server address is required. To change the address, the user first needs to shut down the server.

## tls-profile

<b>Syntax</b>	<b>tls-profile</b> <i>tls-profile-name</i> <b>no tls-profile</b>
<b>Context</b>	config>system>security>ldap>server
<b>Description</b>	This command attaches a TLS client profile to the LDAP client. The parameter in the TLS profile is used to encrypt the LDAP connection to the server. Each LDAP server can use its own TLS profile.

The **no** version of this command removes the TLS profile from LDAP and disables the TLS encryption from LDAP.

**Parameters** *tls-profile-name* — Specifies the TLD profile for encryption.

## timeout

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

**Context** config>system>security>ldap

**Description** The **timeout** value is the number of seconds that the SR OS will wait for a response from the current server that it is trying to establish a connection with. If the server does not reply within the configured **timeout** value, the SR OS will increment the retry counter by 1. The SR OS attempts to establish the connection to the current server up to the configured **retry** value before it moves to the next configured server.

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

**Default** timeout 3

**Parameters** *seconds* — The length of time that the SR OS waits for a response from the server.

**Values** 1 to 90

**Default** 3

## use-default-template

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

**Context** config>system>security>ldap

**Description** This command specifies whether or not the default template is to be actively applied to LDAP.

**Default** use-default-template

## 2.8.2.18 User Management Commands

### user

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

**Context** config>system>security

---

<b>Description</b>	<p>This command creates a local user and a context to edit the user configuration.</p> <p>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.</p> <p>When creating a new user and then entering the <b>info</b> 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 &lt;ENTER&gt; at the password prompt, the user will be logged in.</p> <p>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.</p> <p>The <b>no</b> form of the command deletes the user and all configuration data. Users cannot delete themselves.</p>
<b>Default</b>	none
<b>Parameters</b>	<i>user-name</i> — Specifies the name of the user up to 32 characters.

## access

<b>Syntax</b>	<b>[no] access [ftp] [snmp] [console] [li] [netconf] [grpc]</b>
<b>Context</b>	config>system>security>user config>system>security>user-template
<b>Description</b>	<p>This command grants a user permission for FTP, SNMP, console, lawful intercept (LI), NETCONF, or gRPC 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 this command removes access for a specific application, and 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
<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> — Specifies CLI command access in the lawful intercept (LI) context (applies to the 7450 ESS and 7750 SR).</p>

**netconf** — Specifies NETCONF session access for the user defined in the specified user context. When using the Base-R13 SR OS YANG data model, **console** access is also necessary (not required for the Nokia SR OS YANG data model).

**grpc** — Specifies gRPC access.

## console

<b>Syntax</b>	<b>console</b>
<b>Context</b>	config>system>security>user 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).

## cannot-change-password

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



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

<b>Default</b>	no cannot-change-password
----------------	---------------------------

## login-exec

<b>Syntax</b>	<b>login-exec</b> <i>url-prefix: source-url</i> <b>no login-exec</b>
<b>Context</b>	config>system>security>user>console config>system>security>user-template>console
<b>Description</b>	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

**Parameters** *url-prefix: source-url* — Enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that will be executed after the user successfully logs in.

## member

**Syntax** **member** *user-profile-name* [*user-profile-name.....(up to 8 max)*]  
**no member** *user-profile-name*

**Context** config>system>security>user>console

**Description** This command is used to allow the user access to a profile.

A user can participate in up to eight profiles.

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

**Default** member default

**Parameters** *user-profile-name* — The user profile name up to 32 characters in length.

## new-password-at-login

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

**Context** config>system>security>user>console

**Description** This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login.


The **no** form of the command does not force the user to change passwords.

**Default** no new-password-at-login

## home-directory

**Syntax** **home-directory** *url-prefix* [*directory*] [*directory/directory...*]  
**no home-directory**



<b>Context</b>	config>system>security>user config>system>security>user-template
<b>Description</b>	<p>This command configures the local home directory for the user for both console (file commands and '&gt;' redirection) and FTP access.</p> <p>If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed.</p> <p>The <b>no</b> form of the command removes the configured home directory.</p>
<b>Default</b>	no home-directory
	<p><b>Note:</b> 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.</p>
<b>Parameters</b>	<i>local-url-prefix</i> [ <i>directory</i> ] [ <i>directory/directory...</i> ] — Specifies the user's local home directory URL prefix and directory structure up to 190 characters in length.

## 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> <pre>config&gt;system&gt;security&gt;user# password testuser1</pre> <p>The password is hashed by default.</p> <p>For example:</p> <pre>config&gt;system&gt;security# user testuser1 config&gt;system&gt;security&gt;user\$ password xyzabcd1 config&gt;system&gt;security&gt;user# exit</pre> <pre>config&gt;system&gt;security# info -----</pre>

```

...
        user "testuser1"
        password "$2y$10$pFoehOg/tCbBMPDJ/
kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
        exit
...
-----
config>system>security#

```

The **password** command allows you also to enter the password as a hashed value.

For example:

```

config>system>security# user testuser1
config>system>security>user$ password "$2y$10$pFoehOg/tCbBMPDJ/
kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
config>system>security>user# exit
config>system>security# info
-----
...
user "testuser1"
password "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGy2xsR7WFqyn5fVTnwRzGmOK"
exit
...
-----
config>system>security#

```

**Parameters** *password* — This is the password for the user that must be entered by this user during the login procedure. The minimum length of the password is determined by the **minimum-length** command. The maximum length can be up to 20 chars if unhashed, 32 characters if hashed. The complexity requirements for the password is determined by the **complexity-rules** command and must be followed; otherwise, the password will not be accepted.

All password special characters (#, \$, spaces, and so on) must be enclosed within double quotes.

For example: config>system>security>user# password "south#bay?"

The question mark character (?) cannot be directly inserted as input during a telnet connection because the character is bound to the **help** command during a normal Telnet/console connection.

To insert a # or ? 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).

## public-keys

**Syntax**    **public-keys**

---

<b>Context</b>	config>system>security>user
<b>Description</b>	This command allows the user to enter the context to configure public keys for SSH.

## ecdsa

<b>Syntax</b>	<b>ecdsa</b>
<b>Context</b>	config>system>security>user>public-keys
<b>Description</b>	This command allows the user to enter the context to configure ECDSA public keys.

## ecdsa-key

<b>Syntax</b>	<b>ecdsa-key</b> <i>key-id</i> [ <b>create</b> ] <b>no ecdsa-key</b> <i>key-id</i>
<b>Context</b>	config>system>security>user>public-keys>ecdsa
<b>Description</b>	This command creates an ECDSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.
<b>Parameters</b>	<b>create</b> — Keyword used to create an ECDSA key. The <b>create</b> keyword requirement can be enabled/disabled in the <b>environment&gt;create</b> context. <i>key-id</i> — Specifies the key identifier.
<b>Values</b>	1 to 32

## key-value

<b>Syntax</b>	<b>key-value</b> <i>public-key-value</i> <b>no key-value</b>
<b>Context</b>	config>system>security>user>public-keys>ecdsa>ecdsa-key config>system>security>user>public-keys>rsa>rsa-key
<b>Description</b>	This command configures a value for the RSA or ECDSA public key. The public key must be enclosed in quotation marks. For RSA, the key is between 768 and 4096 bits. For ECDSA, the key is between 1 and 1024 bits.
<b>Default</b>	no key-value
<b>Parameters</b>	<i>public-key-value</i> — Specifies the public key value up to 800 characters in length for RSA and up to 255 characters in length for ECDSA.

---

## rsa

<b>Syntax</b>	<b>rsa</b>
<b>Context</b>	config>system>security>user>public-keys
<b>Description</b>	This command allows the user to enter the context to configure RSA public keys.

## rsa-key

<b>Syntax</b>	<b>rsa-key</b> <i>key-id</i> [ <b>create</b> ] <b>no rsa-key</b> <i>key-id</i>
<b>Context</b>	config>system>security>user>public-keys>rsa
<b>Description</b>	This command creates an RSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.
<b>Parameters</b>	<b>create</b> — Keyword used to create the RSA key. The <b>create</b> keyword requirement can be enabled/disabled in the <b>environment&gt;create</b> context. <i>key-id</i> — Specifies the key identifier. <b>Values</b> 1 to 32

## restricted-to-home

<b>Syntax</b>	<b>[no] restricted-to-home</b>
<b>Context</b>	config>system>security>user config>system>security>user-template
<b>Description</b>	<p>This command prevents users from navigating above their home directories for file access (either by means of CLI sessions with the file command, '&gt;' 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.</p> <p>If a home-directory is not configured or the home directory is not available, then the user has no file access.</p> <p>The <b>no</b> form of the command allows the user access to navigate to directories above their home directory.</p>
<b>Default</b>	no restricted-to-home

## snmp

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

## authentication

<b>Syntax</b>	<b>authentication</b> {[none]   [[hash] {md5 key-1   sha key-1} privacy {none   des-key key-2   aes-128-cfb-key key-2}]} <b>no authentication</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>	no authentication
<b>Parameters</b>	<p><b>none</b> — Do not use authentication. If <b>none</b> is specified, then privacy cannot be configured.</p> <p><b>hash</b> — When <b>hash</b> is not specified, then non-encrypted characters can be entered. When <b>hash</b> is configured, then all specified keys are stored in an encrypted format in the configuration file. The key must be entered in encrypted form when the <b>hash</b> parameter is used.</p> <p><b>md5 key-1</b> — Use an HMAC-MD5-96 authentication key. The MD5 authentication key is stored in an encrypted format. The key must be entered as a full 32 hex character string.</p> <p><b>sha key-1</b> — Use an HMAC-SHA-96 authentication key. The <b>sha</b> authentication key is stored in an encrypted format. The key must be entered as a full 40 hex character string.</p> <p><b>privacy none</b> — Do not perform SNMP packet encryption.</p> <p><b>Default</b>      privacy none</p>

**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.

The **des-key** parameter is not available in FIPS-140-2 mode.

**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 group-name</b> <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 <a href="#">access</a> command links the group with one or more views, security model (s), security level (s), and read, write, and notify permissions
<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.

## user-template

<b>Syntax</b>	<b>user-template {tacplus_default   radius_default   ldap-default}</b>
<b>Context</b>	config>system>security
<b>Description</b>	This command configures default security user template parameters.
<b>Parameters</b>	<p><b>tacplus_default</b> — Specifies the default TACACS+ user template. All parameters of the tacplus_default template except the “profile” are actively applied to all TACACS+ users if tacplus <b>use-default-template</b> is enabled. The “profile” parameters are applied to all TACACS+ users if tacplus authorization is enabled (without the use-priv-lvl option) and tacplus <b>use-default-template</b> is enabled.</p> <p><b>radius_default</b> — Specifies the default RADIUS user template. The radius_default template is actively applied to a RADIUS user if radius authorization is enabled, radius <b>use-default-template</b> is enabled, and no VSAs are returned with the auth-accept from the RADIUS server.</p> <p><b>ldap_default</b> — Specifies the default LDAP user template.</p>

## profile

<b>Syntax</b>	<b>profile</b> <i>user-profile-name</i> <b>no profile</b>
<b>Context</b>	config>system>security>user-template
<b>Description</b>	This command configures the profile for the user based on this template.
<b>Parameters</b>	<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.

## 2.8.2.19 Dot1x Commands

### dot1x

<b>Syntax</b>	[no] <b>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.  The <b>no</b> form of the command removes the 802.1x configuration.

### radius-plcy

<b>Syntax</b>	<b>radius-plcy</b> <i>name</i> [create]
<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.



**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 **config>system>radius** context which authenticates CLI login users who get access to the management plane of the router.

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

---

## retry

<b>Syntax</b>	<b>retry</b> <i>count</i> <b>no retry</b>
<b>Context</b>	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.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	retry 3
<b>Parameters</b>	<i>count</i> — Specifies the retry count.  <b>Values</b> 1 to 10

## server

<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> ]
<b>Context</b>	config>system>security> dot1x>radius-plcy
<b>Description</b>	This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.  Up to five Dot1x servers can be configured at any one time. Dot1x servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other Dot1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.  The <b>no</b> form of the command removes the server from the configuration.
<b>Default</b>	no server
<b>Parameters</b>	<i>server-index</i> — Specifies the index for the Dot1x server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.  <b>Values</b> 1 to 5  <i>ip-address</i> — Specifies the IP address of the Dot1x server. Two Dot1x servers cannot have the same IP address. An error message is generated if the server address is a duplicate.



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

**Values** Up to 128 characters in length.

**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

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

*auth-port* — Specifies a UDP port number to be used as a match criteria.

**Values** 1 to 65535

*server-type* — Specifies the server type.

**Values** authorization, accounting, combined

## source-address

**Syntax** **source-address** *ip-address*

**Context** config>system>security> dot1x>radius-plcy

**Description** This command configures the NAS IP address to be sent in the RADIUS packet.  
The **no** form of the command reverts to the default value.

**Default** By default the System IP address is used in the NAS field.

**Parameters** *ip-address* — Specifies the IP prefix for the IP match criterion in dotted decimal notation.  
**Values** 0.0.0.0 to 255.255.255.255

## shutdown

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

**Context** config>system>security>dot1x  
config>system>security>dot1x>radius-plcy

**Description** This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

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

**Default** shutdown

## timeout

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

**Context** config>system>security> dot1x>radius-plcy

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

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

**Default** timeout 3

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

**Values** 1 to 90

### 2.8.2.20 Keychain Authentication

## keychain

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

**Context** config>system>security

**Description** This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

The **no** form of the command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.

**Default** none

---

<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
<b>Description</b>	This command configures keys for send or receive stream directions.

## entry

<b>Syntax</b>	<b>entry</b> <i>entry-id</i> [ <b>key</b> <i>authentication-key</i>   <i>hash-key</i>   <i>hash2-key</i> ] [ <b>hash</b>   <b>hash2</b> ] <b>algorithm</b> <i>algorithm</i> <b>no entry</b> <i>entry-id</i>
<b>Context</b>	config>system>security>keychain>direction>bi config>system>security>keychain>direction>uni>receive config>system>security>keychain>direction>uni>send
<b>Description</b>	This command defines a particular key in the keychain. Entries are defined by an entry-id. A keychain must have valid entries for the TCP Enhanced Authentication mechanism to work.

The **no** form of the command removes the entry from the keychain. If the entry is the active entry for sending, then this will cause a new active key to be selected (if one is available using the youngest key rule). If it is the only possible send key, then the system will reject the command with an error indicating the configured key is the only available send key.

If the key is one of the eligible keys for receiving, it will be removed. If the key is the only possible eligible key, then the command will not be accepted, and an error indicating that this is the only eligible key will be output.

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

**Default** There are no default entries.

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

**Values** 0 to 63

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

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

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

**Values** A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.

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

**Values** aes-128-cmac-96 — Specifies an algorithm based on the AES standard for TCP authentication.  
hmac-sha-1-96 — Specifies an algorithm based on SHA-1 for RSVP-TE and TCP authentication.  
message-digest — MD5 hash used for TCP authentication.  
hmac-md5 — MD5 hash used for IS-IS and RSVP-TE.  
password — Specifies a simple password authentication for OSPF, IS-IS, and RSVP-TE.  
hmac-sha-1 — Specifies the sha-1 algorithm for OSPF, IS-IS, and RSVP-TE.  
hmac-sha-256 — Specifies the sha-256 algorithm for OSPF and IS-IS.

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

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

**hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

## begin-time

<b>Syntax</b>	<b>begin-time</b> <i>date hours-minutes</i> [UTC] <b>begin-time</b> {now   forever} <b>no begin-time</b>
<b>Context</b>	config>system>security>keychain>direction>bi>entry config>system>security>keychain>direction>uni>receive>entry 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>Default</b>	begin-time forever
<b>Parameters</b>	<i>date hours-minutes</i> — Specifies the date and time for the key to become active.
	<b>Values</b> date: YYYY/MM/DD hours-minutes: hh:mm[:ss]
	<b>now</b> — Specifies the key should become active immediately.
	<b>forever</b> — Specifies that the key should always be inactive.
	<b>UTC</b> — Indicates that time is given with reference to Coordinated Universal Time in the input.

## option

<b>Syntax</b>	<b>option</b> {basic   isis-enhanced} <b>no option</b>
<b>Context</b>	config>system>security>keychain>direction>bi>entry
<b>Description</b>	This command configures allows options to be associated with the authentication key.

- 
- Parameters**
- basic** — 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.
  - isis-enhanced** — 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.

## tolerance

- Syntax**     **tolerance** [*seconds* | **forever**]  
              **no tolerance**
- Context**     config>system>security>keychain>direction>bi>entry  
              config>system>security>keychain>direction>uni>receive>entry
- Description**     This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.
- Parameters**     *seconds* — Specifies the duration that an eligible receive key overlaps with the active send key.
- Values**     0 to 4294967294 seconds
- forever** — Specifies that an eligible receive key overlap with the active send key forever.

## 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.

## 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.

## end-time

<b>Syntax</b>	<b>end-time</b> <i>date hours-minutes</i> [UTC] <b>end-time</b> {now   forever} <b>no end-time</b>
<b>Context</b>	config>system>security>keychain>direction>uni>receive>entry
<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>	end-time 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>

## 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</b> <i>option-number</i> <b>no receive</b>
<b>Context</b>	config>system>security>keychain>tcp-option-number
<b>Description</b>	<p>This command configures the TCP option number accepted in TCP packets received.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>
<b>Default</b>	receive 254

---

**Parameters**    *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

**Values**        253, 254, 253&254, tcp-ao

## send

**Syntax**        **send** *option-number*  
**no send**

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

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

**Default**        send 254

**Parameters**    *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

**Values**        253, 254, tcp-ao

## 2.8.2.21 TTL Security Commands

### ttl-security

**Syntax**        **ttl-security** *min-ttl-value*  
**no ttl-security**

**Context**        config>router>bgp>group  
config>router>bgp>group>neighbor  
config>router>ldp>tcp-session-params>peer-transport  
config>system>login-control>ssh  
config>system>login-control>telnet

**Description**    This command configures TTL security parameters for incoming packets. When the feature is enabled, LDP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of the command disables TTL security.

**Parameters**    *min-ttl-value* — Specifies the minimum TTL value for an incoming BGP packet.

**Values**        1 to 255



---

## 2.8.2.22 gRPC Commands

### grpc

<b>Syntax</b>	<b>grpc</b>
<b>Context</b>	config>system
<b>Description</b>	This command enters the context to configure gRPC parameters.

### allow-unsecure-connection

<b>Syntax</b>	<b>[no] allow-unsecure-connection</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	<p>This command enables unsecure operation of gRPC connections. This means that TCP connections are not encrypted, including username and password information.</p> <p>This command can be enabled only if there is no TLS profile assigned to the gRPC server.</p> <p>The <b>no</b> form of this command enables TLS encryption on gRPC connections.</p>
<b>Default</b>	no allow-unsecure-connection

### gnmi

<b>Syntax</b>	<b>gnmi</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command enables the context for configuring a gNMI service on gRPC.

### auto-config-save

<b>Syntax</b>	<b>[no] auto-config-save</b>
<b>Context</b>	config>system>grpc>gnmi
<b>Description</b>	<p>This command enables automatic saving of the configuration as part of the commit operation.</p> <p>The <b>no</b> form of the command disables automatic saving.</p>

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>grpc>gnmi
<b>Description</b>	This command stops the gNMI service.  The <b>no</b> form of the command starts the gNMI service.

## max-msg-size

<b>Syntax</b>	<b>max-msg-size</b> <i>number</i> <b>no max-msg-size</b>				
<b>Context</b>	config>system>grpc				
<b>Description</b>	This command configures the maximum rx message size that can be received.  The <b>no</b> form of this command reverts to the default.				
<b>Parameters</b>	<i>number</i> — Specifies the message size, in MB. <table><tr><td><b>Values</b></td><td>1 to 1024</td></tr><tr><td><b>Default</b></td><td>512</td></tr></table>	<b>Values</b>	1 to 1024	<b>Default</b>	512
<b>Values</b>	1 to 1024				
<b>Default</b>	512				

## rib-api

<b>Syntax</b>	<b>rib-api</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command enables the context to control the RibAPI gRPC service.

## purge-timeout

<b>Syntax</b>	<b>purge-timeout</b> <i>seconds</i> <b>no purge-timeout</b>
<b>Context</b>	config>system>grpc>rib-api
<b>Description</b>	This command configures the purge timeout associated with the RibApi gRPC service.

If a gRPC client used the RibApi gRPC service to program RIB entries into the router, and then the TCP connection drops for any reason, the associated RIB entries are immediately marked as stale and a timer with the **purge-timeout** value is started. Upon timer expiration, all of the stale entries are removed. While the timer is running, the stale entries remain valid and usable for forwarding but are less preferred than any non-stale entry. The **purge-timeout** gives an opportunity for the disconnected client, or some other client, to re-program the necessary RIB entries so that forwarding can continue uninterrupted.

The **no** form of the command resets to the default value of 0. Entries are immediately deleted when the TCP connection drops.

<b>Default</b>	no purge-timeout
<b>Parameters</b>	<i>seconds</i> — Specifies the number of seconds until the stale entries are purged.
<b>Values</b>	1 to 100 000
<b>Default</b>	0

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>grpc>rib-api
<b>Description</b>	This command stops the RibApi gRPC service, deletes all programmed RIB entries (stale and non-stale), but does not close the TCP connections.  The <b>no</b> form of the command restarts the RibApi gRPC service.

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command stops the gRPC server. This closes all of the associated TCP connections and immediately purges all RIB entries that were programmed using the RibApi Service.  The <b>no</b> form of the command starts the gRPC server.

## tcp-keepalive

<b>Syntax</b>	<b>tcp-keepalive</b>
<b>Context</b>	config>system>grpc

---

**Description** This command enables the context to configure the sending of TCP keepalives by the router towards all gRPC clients.

Enabling TCP keepalive speeds up the detection of certain failures. The TCP keepalives sent by the router are controlled by three commands: **idle-time**, **interval**, and **retries**. The router starts sending TCP keepalives when the connection has been idle (no TCP segments sent or received) for more than **idle-time** seconds. At that point, the router sends a probe (TCP ACK with a sequence number = current sequence number - 1) and expects a TCP ACK. It repeats this probe every **interval** seconds for the configured number of **retries**. If no response is received to any of the probes, the connection is immediately closed, which starts the purge timer if the TCP connection is currently supporting the RibApi service.

## idle-time

**Syntax** **idle-time** *idle*  
**no idle-time**

**Context** config>system>grpc>tcp-keepalive

**Description** This command configures the amount of time in seconds that the connection must be idle before TCP keepalives are sent.

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

**Default** no idle-time

**Parameters** *idle* — Specifies the number of seconds until the first TCP keep-alive probe is sent.

<b>Values</b>	1 to 100 000
<b>Default</b>	600

## interval

**Syntax** **interval** *interval*  
**no interval**

**Context** config>system>grpc>tcp-keepalive

**Description** This command configures the amount of time in seconds between successive TCP keepalive probes sent by the router.

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

**Default** no interval

---

<b>Parameters</b>	<i>interval</i> — Specifies the number of seconds between TCP keepalive probes.
<b>Values</b>	1 to 100 000
<b>Default</b>	15

## retries

<b>Syntax</b>	<b>retries</b> <i>count</i> <b>no retries</b>
<b>Context</b>	config>system>grpc>tcp-keepalive
<b>Description</b>	This command configures the number of TCP keepalive probes sent by the router that must be unacknowledged before the connection is closed.  The <b>no</b> form of the command resets to the default value.
<b>Default</b>	no retries
<b>Parameters</b>	<i>count</i> — Specifies the number of missed keep-alives before the TCP connection is declared down. <b>Values</b> 3 to 100 <b>Default</b> 4

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>grpc>tcp-keepalive
<b>Description</b>	This command stops the TCP keepalives from being sent to all gRPC clients.  The <b>no</b> form of the command restarts the sending of TCP keepalives to all gRPC clients.

## tls-server-profile

<b>Syntax</b>	<b>tls-server-profile</b> <i>name</i> <b>no tls-server-profile</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command adds a configured TLS server profile to the gRPC session. The TLS server is used for encryption of the gRPC session. gRPC will not transmit any PDUs if there is a TLS server profile assigned to it and the TLS connection is down.

The **no** form of the command removes the specified TLS server profile from the gRPC session.

**Parameters**     *name* — Specifies the name of the TLS server profile configured under the **config>system>security>tls** context.

### 2.8.2.23 Login Control Commands

#### login-control

**Syntax**     **login-control**

**Context**     config>system

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

#### exponential-backoff

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

**Context**     config>system>login-control

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

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

**Default**     no exponential-backoff

#### ftp

**Syntax**     **ftp**

**Context**     config>system>login-control

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

#### inbound-max-sessions

**Syntax**     **inbound-max-sessions** *number-of-sessions*  
                 **no inbound-max-sessions**

---

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

## idle-timeout

<b>Syntax</b>	<p><b>idle-timeout</b> {<i>minutes</i>   <b>disable</b>}</p> <p><b>no idle-timeout</b></p>
<b>Context</b>	config>system>login-control
<b>Description</b>	<p>This command configures the idle timeout for console, Telnet, SSH, and FTP sessions before the session is terminated by the system.</p> <p>By default, each idle console, Telnet, SSH, or FTP session times out after 30 minutes of inactivity.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>
<b>Default</b>	idle-timeout 30
<b>Parameters</b>	<p><i>minutes</i> — The idle timeout in minutes. Allowed values are 1 to 1440.</p> <p><b>Values</b>     1 to 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>

## login-banner

<b>Syntax</b>	<b>[no] login-banner</b>
<b>Context</b>	config>system>login-control
<b>Description</b>	<p>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.</p> <p>The <b>no</b> form of the command causes only the configured pre-login-message and a generic login prompt to display.</p>

---

## login-scripts

<b>Syntax</b>	<b>login-scripts</b>
<b>Context</b>	config>system>login-control
<b>Description</b>	This command enables the context to configure CLI scripts that execute when a user (authenticated via any method including local user database, TACACS+, or RADIUS) first logs into a CLI session.

## global

<b>Syntax</b>	<b>global</b> <i>file-url</i> <b>no global</b>
<b>Context</b>	config>system>login-control>login-scripts
<b>Description</b>	<p>This command enables an operator to define a common CLI script that executes when any user logs into a CLI session. This login exec script is executed when any user (authenticated by any means including local user database, TACACS+, or RADIUS) opens a CLI session. This allows a user, for example, to define a common set of CLI aliases that are made available on the router for all users. This global login exec script is executed before any user-specific login exec files that may be configured.</p> <p>This CLI script executes in the context of the user who opens the CLI session. Any commands in the script that the user is not authorized to execute will fail.</p> <p>The <b>no</b> form of this command disables the execution of a global login-script.</p>
<b>Default</b>	no global
<b>Parameters</b>	<i>file-url</i> — The path or directory name.

## per-user

<b>Syntax</b>	<b>per-user user-directory</b> <i>dir-url file-name file-name</i> <b>no per-user</b>
<b>Context</b>	config>system>login-control>login-scripts
<b>Description</b>	<p>This command allows users to define their own login scripts that can be executed each time they first login to a CLI session. The command executes the script "<i>file-url / username / file-name</i>" when the user <i>username</i> logs into a CLI session (authenticated by any means including local user database, TACACS+, or RADIUS).</p> <p>For example:</p> <p>per-user user-directory "cf1:/local/users" file-name "login-script.txt"</p>



would search for the following script when user “admin” logs in and authenticates via RADIUS:

```
cf1:/local/users/admin/login-script.txt
```

The per user login script is executed after any global script executes and before any login-exec script configured against a local user is executed. This allows users, for example, who are authenticated via TACACS+ or RADIUS to define their own login scripts.

This CLI script executes in the context of the user who opens the CLI session. Any commands in the script that the user is not authorized to execute will fail.

The **no** form of the command disables the execution of any per user login-scripts.

<b>Default</b>	no per-user
<b>Parameters</b>	<p><i>dir-url</i> — Specifies the path or directory name.</p> <p><i>file-name</i> — Specifies the name of the file (located in the <i>dir-url</i> directory) including the extension.</p>

## motd

<b>Syntax</b>	<b>motd</b> { <i>url url-prefix: source-url</i>   <b>text</b> <i>motd-text-string</i> }
	<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 motd
<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> — Specifies 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 can be used to create multi-line messages. A \n in the message moves to the beginning of the next line by sending ASCII/UTF-8 chars 0xA (LF) and 0xD (CR) to the client terminal. An \r in the message sends the ASCII/UTF-8 char 0xD (CR) to the client terminal.</p>

---

## pre-login-message

<b>Syntax</b>	<b>pre-login-message</b> <i>login-text-string</i> [ <b>name</b> ] <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.</p> <p>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 pre-login-message
<b>Parameters</b>	<p><i>login-text-string</i> — Specifies the login text string up to 900 characters in length. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes. Some special characters can be used to format the message text. The \n character can be used to create multi-line messages. A \n in the message moves to the beginning of the next line by sending ASCII/UTF-8 chars 0xA (LF) and 0xD (CR) to the client terminal. A \r in the message sends the ASCII/UTF-8 char 0xD (CR) to the client terminal.</p> <p><b>name</b> — When this keyword is specified, 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 config>system>security
<b>Description</b>	This command enables the context to configure the SSH parameters.

## 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.

---

## 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.  The <b>no</b> form of the command disables graceful shutdown of SSH sessions.

## inbound-max-sessions

<b>Syntax</b>	<b>inbound-max-sessions</b> <i>number-of-sessions</i> <b>no inbound-max-sessions</b>
<b>Context</b>	config>system>login-control>telnet config>system>login-control>ssh
<b>Description</b>	This parameter limits the number of inbound Telnet and SSH sessions. A maximum of 30 telnet and ssh connections can be established to the router. The local serial port cannot be disabled.  Telnet and SSH maximum sessions can also use the combined total of both inbound sessions (SSH+Telnet). While it is acceptable to continue to internally limit the combined total of SSH and Telnet sessions to N, either SSH or Telnet sessions can use the inbound maximum sessions, if so required by the Operator.  The <b>no</b> form of the command reverts to the default value.
<b>Default</b>	inbound-max-sessions 5
<b>Parameters</b>	<i>number-of-sessions</i> — The maximum number of concurrent inbound Telnet sessions, expressed as an integer.  <b>Values</b> 0 to 50 (default = 5) or 0 to N where N is the new total number of SSH+Telnet sessions if they are scaled

## outbound-max-sessions

<b>Syntax</b>	<b>outbound-max-sessions</b> <i>number-of-sessions</i> <b>no outbound-max-sessions</b>
<b>Context</b>	config>system>login-control>telnet config>system>login-control>ssh
<b>Description</b>	This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled.

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

**Default** outbound-max-sessions 5

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

**Values** 0 to 15

## enable-graceful-shutdown

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

**Context** config>system>login-control>telnet

**Description** This command enables graceful shutdown of telnet sessions.

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

## 2.9 Security Show, Clear, Debug, Tools, and Admin Command Reference

### 2.9.1 Command Hierarchies

- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)
- [Tools Commands](#)
- [Admin Commands](#)

#### 2.9.1.1 Show Commands

##### 2.9.1.1.1 System Security

```

show
  — system
    — connections [detail] [address ip-address] [port port-number]
    — grpc
    — grpc connection
    — grpc rpc [rpc-id]
    — security
      — access-group [group-name]
      — authentication [statistics]
      — cli-session-group
      — cpm-filter
        — ip-filter [entry entry-id]
        — ipv6-filter [entry entry-id]
        — mac-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-filter [entry entry-id]
        — mac-filter [entry entry-id]
    — password-options
    — per-peer-queuing [detail]
    — per-peer-queuing
    — profile [user-profile-name]
    — source-address
    — ssh [detail]
    — user [user-name] [detail]
    — user [user-name] lockout
    — view [view-name] [detail]
— certificate
    — ca-profile
    — ca-profile name [association]
    — oosp-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]

```

### 2.9.1.1.2 Login Control

```

show
  — users

```

### 2.9.1.2 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-filter** *[entry entry-id]*
    - **mac-filter** *[entry entry-id]*
  - **cpu-protection**
    - **excessive-sources**
    - **protocol-protection**
    - **violators** *[port] [interface] [sap]*
  - **cpm-queue** *queue-id*
- admin
- user
    - user
      - **lockout** *{name | all}*
      - **password-history** *{name | all}*

### 2.9.1.3 Debug Commands

- debug
- **certificate**
    - *[no]* **ocsp**
      - *[no]* **ca-profile** *profile-name*
  - **radius** *[detail] [hex]*
  - **no radius**
  - **system**
    - *[no]* **grpc**
      - **client** *all*
      - **client** *ip-address*
      - **no client**
      - **type** *all*
      - **type** *[gnmi-capabilities] [gnmi-get] [gnmi-set] [gnmi-subscribe]*
      - **no type**

### 2.9.1.4 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]*

### 2.9.1.5 Admin Commands

```
admin
— clear
  — lockout {user user-name | all}
  — password-history {user user-name | all}
```

### 2.9.2 Command Descriptions

- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)
- [Tools Commands](#)
- [Admin Commands](#)



## 2.9.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

### 2.9.2.1.1 System Commands

#### connections

<b>Syntax</b>	<b>connections</b> [ <b>detail</b> ] [ <b>address</b> <i>ip-address</i> ] [ <b>port</b> <i>port-number</i> ]
<b>Context</b>	show>system
<b>Description</b>	This command displays TCP connections and UDP listeners.
<b>Parameters</b>	<b>detail</b> — Displays detail connection information <i>ip-address</i> — Specifies the IPv4 or IPv6 address <b>Values</b> <i>ip-int-name</i> - 32 chars max <i>ipv4-address</i> - a.b.c.d <i>ipv6-address</i> - x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D <i>port-number</i> — Specifies the port number <b>Values</b> 0 to 65535
<b>Output</b>	The following is an example of system connections information.

#### Sample Output

```
*A:cses-V22# show system connections detail
=====
Connections (Detail)
=====
Prot RecvQ  TxmtQ   Local Address                      State
      MSS   Remote Address                      vRtrID
-----
TCP      0      0 0.0.0.0.22                          LISTEN
      1024 0.0.0.0.0                          0
TCP      0      0 0.0.0.0.6068                        LISTEN
      1024 0.0.0.0.0                          0
TCP      0      0 0.0.0.0.47806                       LISTEN
      1024 0.0.0.0.0                          0
TCP      0      0 ::.22                              LISTEN
      1024 ::.0                              0
```

```

TCP      0      0  ::.47806                                LISTEN
      1024  ::.0                                0
TCP      0      0  127.0.0.1.49511                            ESTABLISH
      8192  127.0.0.1.49512                            4095
TCP      0      0  127.0.0.1.49512                            ESTABLISH
      8192  127.0.0.1.49511                            4095
TCP      0      2  127.0.0.1.49513                            ESTABLISH
      8192  127.0.0.1.49514                            4095
TCP     163      0  127.0.0.1.49514                            ESTABLISH
      8192  127.0.0.1.49513                            4095
TCP      0      0  127.1.0.11.21                               LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  127.1.0.11.21059                           LISTEN
      1024  0.0.0.0.0                                4095
TCP      0      0  135.227.236.22.22                           LISTEN
      1024  0.0.0.0.0                                4095
TCP      0     2256 135.227.236.22.22                       ESTABLISH
      1024  135.244.40.224.65066                       4095
UDP      0      0  0.0.0.0.67                                  ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.68                                  ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.319                                 ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.320                                 ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.50700                               ---
      0.0.0.0.0                                0
UDP      0      0  0.0.0.0.50702                               ---
      0.0.0.0.0                                0
UDP      0      0  ::.50701                                    ---
      ::.0                                        0
UDP      0      0  ::.50703                                    ---
      ::.0                                        0
UDP      0      0  0.0.0.0.1025                                ---
      0.0.0.0.0                                1
UDP      0      0  ::.1025                                     ---
      ::.0                                        1
UDP      0      0  0.0.0.0.49152                               ---
      0.0.0.0.0                                4095
UDP      0      0  127.1.0.11.69                               ---
      0.0.0.0.0                                4095

```

-----  
No. of Connections: 25  
-----

TCP Statistics  
-----

```

packets sent                : 15349
data packets                : 11627 (230636 bytes)
data packet retransmitted   : 0 (0 bytes)
ack-only packets            : 3691 (19 delayed)
URG only packet              : 0
window probe packet         : 0
window update packet        : 7
control packets              : 24
packets received             : 15390
acks                        : 4148 for (230443 bytes)
duplicate acks               : 473
ack for unsent data          : 0

```

```
packets received in-sequence      : 11007 (170236 bytes)
completely duplicate packet       : 0 (0 bytes)
packet with some dup. data        : 0 (0 bytes)
out-of-order packets             : 0 (0 bytes)
packet of data after window       : 0 (0 bytes)
window probe                     : 0
window update packet             : 0
packets received after close      : 5
discarded for bad checksum        : 0
discarded for bad header offset field : 0
discarded because packet too short : 0
packets dropped by md5            : 0
packets dropped by enhanced auth  : 0
packets dropped by tcp-ao         : 0
connection request               : 9
connection accept                : 11
connections established (including accepts) : 20
connections closed               : 24 (including 5 drops)
embryonic connections dropped    : 0
segments updated rtt             : 3617 (of 3612 attempts)
retransmit timeouts              : 0
connections dropped by rexmit timeout : 0
persist timeouts                : 0
keepalive timeouts               : 481
keepalive probes sent           : 470
connections dropped by keepalive  : 1
connections dropped by full queue : 0
pcb cache lookups failed         : 12
path mtu discovery backoff       : 0
=====
*A:cses-V22#
```

## grpc

<b>Syntax</b>	<b>grpc</b> <b>grpc connection</b> <b>grpc rpc</b> [ <i>rpc-id</i> ]
<b>Context</b>	show>system
<b>Description</b>	This command displays gRPC server information.
<b>Parameters</b>	<b>connection</b> — This command displays information for gRPC connections. <i>rpc-id</i> — Specifies an rpc ID. <b>Values</b> 0 to 4294967295

**Output** The following is an example of system gRPC information.

[Table 32](#) describes system gRPC output fields.

### Sample Output

```
A:admin@Dut-A# show system grpc
```

```

=====
gRPC Server
=====
Administrative State      : Enabled
Operational State        : Up
Supported services
-----
gNMI Version              : 0.4.0
=====

A:admin@Dut-A# show system grpc connection
=====
gRPC Server connections
=====
Address                   : 192.99.5.0
Port                      : 49648
Establishment Time        : 2018/02/20 09:51:48
Active RPC Count          : 0
Total RPC Count           : 1
Rx Bytes                  : 2954
Tx Bytes                  : 3908
-----
No. of connections        : 1
=====

A:node-6>show>system# grpc rpc
=====
gRPC Server RPCs
=====
No. of RPCs               : 0
=====

```

**Table 32** Show System gRPC Output Fields

Label	Description
gRPC Server	Specifies the gRPC server name.
Administrative State	Specifies the administrative state (Enabled, Disabled).
Operational State	Specifies the operational state (Up, Down).
Supported services	Specifies the supported services.
gNMI Version	Specifies the gNMI version.
Address	Specifies the IP address.
Port	Specifies the port number.
Establishment Time	Specifies the establishment time.

**Table 32 Show System gRPC Output Fields (Continued)**

Label	Description
Active RPC Count	Specifies the active RPC count.
Total RPC Count	Specifies the total RPC count.
Rx Bytes	Specifies the number of received bytes.
Tx Bytes	Specifies the number of transmitted bytes.
No. of connections	Specifies the number of gRPC connections.
No. of RPCs	Specifies the number of RPCs.

### 2.9.2.1.2 Security Commands

#### access-group

**Syntax** `access-group [group-name]`

**Context** `show>system>security`

**Description** This command displays SNMP access group information.

**Parameters** *group-name* — This command displays information for the specified access group.

**Output** The following is an example of access group information.

[Table 33](#) describes security access group output fields.

#### Sample Output

```
A:ALA-4# show system security access-group
=====
Access Groups
=====
group name      security  security  read      write      notify
                model    level    view      view      view
-----
snmp-ro         snmpv1   none     no-security          no-security
snmp-ro         snmpv2c  none     no-security          no-security
snmp-rw         snmpv1   none     no-security  no-security  no-security
snmp-rw         snmpv2c  none     no-security  no-security  no-security
snmp-rwa        snmpv1   none     iso          iso          iso
snmp-rwa        snmpv2c  none     iso          iso          iso
snmp-trap       snmpv1   none     iso          iso          iso
snmp-trap       snmpv2c  none     iso          iso          iso
```

=====

A:ALA-7#

**Table 33      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.

authentication

- Syntax**      **authentication [statistics]**
- Context**      show>system>security
- Description**      This command displays system login authentication configuration and statistics.
- Parameters**      **statistics** — Appends login and accounting statistics to the display.
- Output**      The following is an example of authentication information.

[Table 34](#) describes system security authentication output fields.

**Sample Output**

```
A:ALA-4# show system security authentication
=====
Authentication          sequence : radius tacplus local ldap exit-on-reject
=====
type                    status  timeout (secs)  retry count
  server address
  server name
-----
radius                  down    3                3
  192.168.255.255
  n/a
ldap                    up      3                3
  192.168.0.10(389)
  my_first_LDAP_server
```

```

ldap                                down      3              3
  10.0.0.0(389)
  n/a
-----
radius admin/oper status   : up/down
ldap admin/oper status    : up/up
health check               : enabled (interval 30 secs)
-----
No. of Servers: 3
=====

```

```

A:ALA-4# show system security authentication statistics
=====
Authentication               sequence : radius tacplus ldap local
=====
type                          status      timeout (secs)  retry count
  server address
  server name
-----
ldap                          down        3              3
  10.20.194.179:10390
  n/a
-----
ldap admin/oper status      : down/down
health check                : enabled (interval 30 secs)
-----
No. of Servers: 1
=====

```

```

Login Statistics
=====
server address                conn  accepted  rejected
                              errors logins   logins
-----
135.243.194.179              0     2         7
local                         n/a    10        8
=====

```

```

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

```

```

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

```

```

A:ALA-4# show system security authentication
=====
Authentication               sequence : radius tacplus local ldap exit-on-reject
=====
type                          status    timeout (secs)  retry count
  server address
  server name
-----

```

```

radius                                up      5      5
  10.10.10.103
  n/a
radius                                up      5      5
  10.10.10.1
  n/a
radius                                up      5      5
  10.10.10.2
  n/a
radius                                up      5      5
  10.10.10.3
  n/a
-----
radius admin status   : up
tacplus admin status : up
health check         : enabled (interval 30)
-----
No. of Servers: 4
=====
A:ALA-4#

A:ALA-7>show>system>security# authentication statistics
=====
Authentication                sequence : radius tacplus local
=====
type                           status  timeout (secs)  retry count
server address
-----
radius                          up      5      5
  10.10.10.103
radius                          up      5      5
  10.10.10.1
radius                          up      5      5
  10.10.10.2
radius                          up      5      5
  10.10.10.3
-----
radius admin status   : up
tacplus admin status : up
health check         : enabled (interval 30)
-----
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 (secs)  retry count
server address
-----
radius                  up      5                5
10.10.10.103
radius                  up      5                5
10.10.10.1
radius                  up      5                5
10.10.10.2
radius                  up      5                5
10.10.10.3
-----
radius admin status    : up
tacplus admin status   : up
health check           : enabled (interval 30)
-----
No. of Servers: 4
=====

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
=====

```

**Table 34** 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.
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.

## cli-session-group

- Syntax** **cli-session-group** *session-group-name*
- Context** show>system>security
- Description** This command displays the user profiles of this CLI session group and the session group details.
- Parameters** *session-group-name* — Specifies a session group, up to 32 characters.

## policy

- Syntax** **policy** [*policy-id*] **association**
- Context** show>system>security>cpu-protection  
show>system>security>dist-cpu-protection
- Description** This command displays CPU protection policy information.
- Parameters** *policy-id* — Displays CPU protection policy information for the specified policy ID.

**association** — This keyword displays associations for the specified policy ID.

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 [entry <i>entry-id</i>]</b>
<b>Context</b>	show>system>security>cpm-filter
<b>Description</b>	This command displays CPM IP filters.
<b>Parameters</b>	<i>entry-id</i> — Identifies a CPM filter entry as configured on this system. <b>Values</b> 1 to 6144
<b>Output</b>	The following displays IP filter entry information.

[Table 35](#) describes CPM IP filter output fields.

**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#

```

**Table 35** 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.

**Table 35 Show CPM IP Filter Output Fields (Continued)**

Label	Description
TCP-ack	Displays the ACK flag in the TCP header
Match action	When the criteria matches, displays drop or forward packet.
Next Hop	In case match action is forward, indicates destination of the matched packet.
Dropped pkts	Indicates number of matched dropped packets
Forwarded pkts	Indicates number of matched forwarded packets.

## ipv6-filter

**Syntax** `ipv6-filter [entry entry-id]`

**Context** `show>system>security>cpm-filter`

**Description** This command displays CPM IPv6 filters and only applies to the 7750 SR and 7950 XRS.

**Parameters** *entry-id* — Identifies a CPM IPv6 filter entry as configured on this system.

**Values** 1 to 6144

**Output** The following displays an example of IPv6 filter entry information.

[Table 36](#) describes CPM IPv6 filter output fields.

**The following is an output example on the 7750 SR:**

```
A:ALA-35# show system security cpm-filter ipv6-filter
=====
CPM IPv6 Filters
=====
Entry-Id Dropped Forwarded Description
-----
101      25880    0      CPM-Filter 2001:db8::101:2 #101
102      25880    0      CPM-Filter 2001:db8::102:2 #102
103      25880    0      CPM-Filter 2001:db8::103:2 #103
104      25880    0      CPM-Filter 2001:db8::104:2 #104
105      25880    0      CPM-Filter 2001:db8::105:2 #105
106      25880    0      CPM-Filter 2001:db8::106:2 #106
107      25880    0      CPM-Filter 2001:db8::107:2 #107
108      25880    0      CPM-Filter 2001:db8::108:2 #108
109      25880    0      CPM-Filter 2001:db8::109:2 #109
=====
A:ALA-35#

A:ALA-35# show system security cpm-filter ipv6-filter entry 101
=====
```

```

CPM IPv6 Filter Entry
=====
Entry Id : 1
Description : CPM-Filter 2001:db8::101:2 #101
-----
Filter Entry Match Criteria :
-----
Log Id : n/a
Src. IP : 2001:db8::101:2      Src. Port : 0
Dest. IP : 2001:db8::101:1    Dest. Port : 0
next-header : none           Dscp : Undefined
ICMP Type : Undefined        ICMP Code : Undefined
TCP-syn : Off                TCP-ack : Off
Match action : Drop
Dropped pkts : 25880          Forwarded pkts : 0
=====
A:ALA-35#

```

**Table 36** Show CPM IPv6 Filter Output Fields

Label	Description
Entry-Id	Displays information about the specified management access filter entry
Dropped	Displays the number of dropped events.
Forwarded	Displays the number of forwarded events.
Description	Displays the CPM filter description.
Log ID	Log Id where matched packets will be logged.
Src IP	Displays Source IP address(/netmask)
Dest. IP	Displays Destination IP address(/netmask).
Src Port	Displays Source Port Number (range).
Dest. Port	Displays Destination Port Number (range).
next-header	Displays next-header field in the IPv6 header.
Dscp	Displays Traffic Class field in the IPv6 header.
ICMP Type	Displays ICMP type field in the icmp header.
ICMP Code	Displays ICMP code field in the icmp header.
TCP-syn	Displays the SYN flag in the TCP header.
TCP-ack	Displays the ACK flag in the TCP header
Match action	When criteria matches, displays drop or forward packet.
Next Hop	In case match action is forward, indicates destination of the matched packet.

**Table 36 Show CPM IPv6 Filter Output Fields (Continued)**

Label	Description
Dropped pkts	Indicating number of matched dropped packets
Forwarded pkts	Indicating number of matched forwarded packets.

## 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>	<i>entry-id</i> — Displays information about the specified entry. <b>Values</b> 1 to 2048
<b>Output</b>	The following is an output example of CPU MAC filter information.

### 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#
```

## cpm-queue

<b>Syntax</b>	<b>cpm-queue</b> <i>queue-id</i>
<b>Context</b>	show>system>security
<b>Description</b>	This command displays CPM queues.
<b>Parameters</b>	<i>queue-id</i> — Specifies an integer value that identifies a CPM queue. <b>Values</b> 0, 33 to 2000
<b>Output</b>	The following display CPM IPv6 filter information.

[Table 37](#) describes CPM queue output fields.

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#
```

Table 37      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.

cpu-protection

- Syntax**      **cpu-protection**
- Context**     show>system>security
- Description**    This command enables the context to display CPU protection information.
- Output**        The following output is an example of ETH CFM monitoring.

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 First-Time	Level 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		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 First-Time	Level 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	3000000007
1:2	3					
255	max			05/01/2010 01:43:55	06/27/2010 22:37:23	3000000008
1:3	3					
100	61234			05/01/2010 01:43:57	06/27/2010 22:37:26	3000000009
1:4	3					
255	max			05/01/2010 01:43:59	06/27/2010 22:37:29	3000000010
1:5	3					
100	61234			05/01/2010 01:44:01	06/27/2010 22:37:32	3000000011

-----

5 SDP('s) found  
=====

```

show system security cpu-protection excessive-sources
=====
SAP's where the protection policy per-source rate limit is exceeded
=====
SAP-Id                               Service-Id
  Plcy Limit
-----
1/1/1                                3
  100  65534
-----
1 SAP('s) found
=====
SDP's where the protection policy per-source rate limit is exceeded
=====
SDP-Id          Service-Id  Plcy  Limit
-----
1:3              3          100   65534
1:4              3          255   max
1:5              3          100   65534
-----
3 SDP('s) found
=====

show system security cpu-protection policy association
=====
Associations for CPU Protection policy 100
=====
Description : (Not Specified)
SAP associations
-----
Service Id   : 3                               Type   : VPLS
  SAP 1/1/1                               mac-monitoring
  SAP 1/1/2                               eth-cfm-monitoring aggr car
  SAP 1/1/3                               eth-cfm-monitoring
  SAP 1/1/4
-----
Number of SAP's : 4
SDP associations
-----
Service Id   : 3                               Type   : VPLS
  SDP 1:1                               eth-cfm-monitoring aggr car
  SDP 1:3                               eth-cfm-monitoring aggr
  SDP 1:5                               mac-monitoring
  SDP 17407:4123456789                 eth-cfm-monitoring car
-----
Number of SDP's : 4
Interface associations
-----
None
Managed SAP associations
-----
None
Video-Interface associations
-----
None
=====
Associations for CPU Protection policy 254

```

```
=====
Description : Default (Modifiable) CPU-Protection Policy assigned to Access
                Interfaces
SAP associations
-----
None
SDP associations
-----
None
Interface associations
-----
Router-Name : Base
                ies6If
Router-Name : vprn7
                vprn If
-----
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:bk sim130#

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
100 61234 05/01/2010 01:43:41 06/27/2010 22:37:02 30000000001
-----
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 30000000001
1:2              3
255 max 05/01/2010 01:43:43 06/27/2010 22:37:05 30000000002
1:3              3
100 61234 05/01/2010 01:43:45 06/27/2010 22:37:08 30000000003
1:4              3
255 max 05/01/2010 01:43:47 06/27/2010 22:37:11 30000000004
1:5              3
100 61234 05/01/2010 01:43:49 06/27/2010 22:37:14 30000000005
-----
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

**Syntax** `eth-cfm-monitoring [{service-id service-id sap-id sap-id} | {service-id service-id sdp-id sdp-id:vc-id}]`

**Context** `show>system>security>cpu-protection`

**Description** This command displays sources exceeding their eth-cfm-monitoring rate limit.

**Parameters** *service-id* — Specifies the service ID.

**Values** 1 to 2148278317, svc-name up to 64 characters in length

## excessive-sources

**Syntax** `excessive-sources [service-id service-id sap-id sap-id]`

**Context** `show>system>security>cpu-protection`

**Description** This command displays sources exceeding their per-source rate limit.

**Parameters**     *service-id* — Displays information for services exceeding their per-source rate limit.  
                       *sap-id* — Displays information for SAPs exceeding their per-source rate limit.

## protocol-protection

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

## violators

**Syntax**            **violators [port] [interface] [sap] [video] [sdp]**  
**Context**           show>system>security>cpu-protection  
**Description**       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.  
**Parameters**       **port** — Displays violators associated with the port.  
                       **interface** — Displays violators associated with the interface.  
                       **sap** — Displays violators associated with the SAP.  
                       **video** — Displays violators associated with the video entity.  
                       **sdp** — Displays violators associated with the SDP.  
**Output**            The following is an output example of CPU protection violators.

### 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
=====
```

dist-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 Distributed CPU Protection information.

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. <b>detail</b> — Displays detailed keychain information.
<b>Output</b>	The following is an output example of 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 to 9999

**Output**        The following is an output example of MAF IP filter information

[Table 38](#) describes management access filter output fields.

**Sample Output**

```
*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#
```

**Table 38**        **Show Management Access Filter Output Fields**

Label	Description
Def. action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted. Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued. Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied.
Entry	The entry ID in a policy or filter table.
Description	A text string describing the filter.
Src IP	The source IP address used for management access filter match criteria.
Src interface	The interface name for the next hop to which the packet should be forwarded if it hits this filter entry.
Dest port	The destination port.

**Table 38 Show Management Access Filter Output Fields (Continued)**

Label	Description
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.

## ipv6-filter

<b>Syntax</b>	<b>ipv6-filter</b> [ <b>entry</b> <i>entry-id</i> ]
<b>Context</b>	show>system>security>mgmt-access-filter
<b>Description</b>	This command displays management-access IPv6 filters and only applies to the 7750 SR and 7950 XRS.
<b>Parameters</b>	<i>entry-id</i> — Specifies the IPv6 filter entry ID to display. <b>Values</b> 1 to 9999
<b>Output</b>	The following is an output example of MAF IPv6 filter information

### Sample Output

```
*A:Dut-C# show system security management-access-filter ipv6-filter entry 1
=====
IPv6 Management Access Filter
=====
filter type      : ipv6
Def. Action      : permit
Admin Status     : enabled (no shutdown)
-----
Entry            : 1
Src IP           : 2001:db8::1/128
Flow label       : undefined
Src interface    : undefined
Dest port        : undefined
Next-header      : undefined
Router           : undefined
Action           : permit
Log              : enabled
Matches         : 0
=====
*A:Dut-C# s
```

mac-filter

<b>Syntax</b>	<b>mac-filter</b> [ <b>entry</b> <i>entry-id</i> ]
<b>Context</b>	show>system>security>mgmt-access-filter
<b>Description</b>	This command displays management access MAC filters.
<b>Parameters</b>	<i>entry-id</i> — Displays information about the specified entry. <b>Values</b> 1 to 9999

**Output**

**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#
```

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>	The following is an example of password options information.

[Table 39](#) describes password options output fields.

**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#
```

**Table 39 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.
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.

**Table 39 Show Password Options Output Fields (Continued)**

Label	Description
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 username	Displays whether the user name is allowed as part of the password.
Palindrome allowed	Displays whether palindromes are allowed as part of the password.

## per-peer-queuing

- Syntax** `per-peer-queuing [detail]`
- Context** `show>system>security`
- Description** This command enables or disables CPMCFM hardware queuing per peer. TTL security only operates when per-peer-queuing is enabled.
- Output** The following is an example of per peer queuing information.

[Table 40](#) describes per-peer-queuing output fields.

### 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
```

**Table 40** 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.

## 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** The following is an example of user profile output information.

[Table 41](#) describes user profile output fields.

### Sample Output

```
A:ALA-7# show system security profile administrative
=====
User Profile
=====
User Profile : administrative
Def. Action  : permit-all
-----
Entry       : 10
Description :
Match Command: configure system security
Action      : permit
-----
Entry       : 20
Description :
Match Command: show system security
Action      : permit
-----
```

```
No. of profiles:
=====
A:ALA-7#
```

**Table 41**      **Show User Profile Output Fields**

Label	Description
User Profile	Displays the profile name used to deny or permit user console access to a hierarchical branch or to specific commands.
Def. action	Permit all — Permits access to all commands. Deny — Denies access to all commands. None — No action is taken.
Entry	The entry ID in a policy or filter table.
Description	Displays the text string describing the entry.
Match Command	Displays the command or subtree commands in subordinate command levels.
Action	Permit all — Commands matching the entry command match criteria are permitted. Deny — Commands not matching the entry command match criteria are not permitted.
No. of profiles	The total number of profiles listed.

source-address

- Syntax**      **source-address**
- Context**      show>system>security
- Description**      This command displays source-address configured for applications.
- Output**      The following is an example of source address output information.

[Table 42](#) describes source address output fields.

**Sample Output**

```
A:SR-7# show system security source-address
=====
Source-Address applications
=====
Application          IP address/Interface Name          Oper status
-----
telnet               10.20.1.7                          Up
radius              loopback1                          Up
```



```
=====
A:SR-7#
```

**Table 42 Show Source Address Output Fields**

Label	Description
Application	Displays the source-address application.
IP address Interface Name	Displays the source address IP address or interface name.
Oper status	Up: The source address is operationally up. Down: The source address is operationally down.

## ssh

<b>Syntax</b>	<b>ssh</b>
<b>Context</b>	show>system>security
<b>Description</b>	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.
<b>Output</b>	The following is an example of SSH output information.

[Table 43](#) describes SSH output fields

### Sample output

```
A:dut-c# show system security ssh
=====
SSH Server
=====
Administrative State      : Enabled
Operational State        : Up
Preserve Key              : Disabled
Key-re-exchange           : 60 minutes / 1024 MB

SSH Protocol Version 1    : Disabled

SSH Protocol Version 2    : Enabled
DSA Host Key Fingerprint  : b2:9f:d6:b7:fa:f4:dc:7b:cc:a8:97:46:80:4c:f3:7a
RSA Host Key Fingerprint  : cd:43:17:59:7f:17:f8:64:c6:a8:51:9c:99:44:0f:d4

-----
Connection                Username
  Version  Cipher          ServerName  Status
Router Ins  MAC              Key-re-exchange
-----
10.20.142.155              admin
```

```

      2      aes128-ctr      cli      connected
management  hmac-md5      60 minutes / 1024 MB
10.10.18.2
      2      aes128-ctr      admin
Base        hmac-md5      cli      connected
                                15 minutes / 512 MB
-----
Number of SSH sessions : 2
=====

```

**Table 43** Show System Security SSH Options Output Fields

Label	Description
Administrative State	Enabled: The SSH server is enabled. Disabled: The SSH server is disabled.
Operational State	Up: The SSH server is up. Down: The SSH server is down.
Preserve Key	Enabled: The preserve-key is enabled. Disabled: The preserve-key is disabled.
Key-re-exchange	Displays the maximum time elapsed and maximum mbytes transmitted before a key re-exchange is initiated. All new sessions will be created with this value.
SSH protocol version 1	Enabled: SSH1 is enabled. Disabled: SSH1 is disabled.
SSH protocol version 2	Enabled: SSH2 is enabled. Disabled: SSH2 is disabled.
DSA Host 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.
RSA Host 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 cannot continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected routers (remote client).
Username	The name of the user.
Version	The SSH version number.

**Table 43 Show System Security SSH Options Output Fields (Continued)**

Label	Description (Continued)
Cipher	<p>3des: A SSHv1 encryption method that allows proprietary information to be transmitted over untrusted networks.</p> <p>3des-cbc: A SSHv2 encryption method.</p> <p>aes128-cbc: A SSHv2 128-bit encryption method.</p> <p>aes128-ctr: A SSHv2 128-bit encryption method.</p> <p>aes192-cbc: A SSHv2 192-bit encryption method.</p> <p>aes192-ctr: A SSHv2 192-bit encryption method.</p> <p>aes256-cbc: A SSHv2 256-bit encryption method.</p> <p>aes256-ctr: A SSHv2 256-bit encryption method.</p> <p>arcfour: A SSHv2 encryption method.</p> <p>des: A SSHv1 encryption method using a private (secret) key.</p> <p>blowfish: A SSHv1 encryption method.</p> <p>blowfish-cbc: A SSHv2 encryption method.</p> <p>cast128-cbc: A SSHv2 1280-bit encryption method.</p> <p>rijndael-cbc: A SSHv2 encryption method.</p>
Server Name	The server name.
Status	<p>connected: The SSH connection is connected.</p> <p>disconnected: The SSH connection is disconnected.</p>
Router Ins	SSH server router instance. Can be the router name ("Base" or "management") or the VPRN Id (1 to 2147483647).
MAC	<p>hmac-sha2-512: The SSH MAC algorithm used is hmac-sha2-512.</p> <p>hmac-sha2-256: The SSH MAC algorithm used is hmac-sha2-256.</p> <p>hmac-sha1: The SSH MAC algorithm used is hmac-sha1.</p> <p>hmac-sha1-96: The SSH MAC algorithm used is hmac-sha1-96.</p> <p>hmac-md5: The SSH MAC algorithm used is hmac-md5.</p> <p>hmac-ripemd160: The SSH MAC algorithm used is hmac-ripemd160.</p> <p>hmac-sha2-512: The SSH MAC algorithm used is hmac-sha2-512.</p> <p>hmac-ripemd160-openssh-com: The SSH MAC algorithm used is hmac-ripemd160-openssh-com.</p>
Key-re-exchange	Maximum time elapsed and maximum mbytes transmitted before a key re-exchange is initiated for this session.

**Table 43      Show System Security SSH Options Output Fields (Continued)**

Label	Description (Continued)
Number of SSH sessions	The total number of SSH sessions.

The following is an example of SSH detail output information.

Table 44 describes SSH detail output fields

**Sample output**

```
*A:dut-a# show system security ssh detail
=====
SSH Server Global
=====
Administrative State      : Enabled
Operational State        : Up
Preserve Key              : Disabled
Key-re-exchange          : 60 minutes / 1024 MB
SSH Protocol Version 1    : Disabled
SSH Protocol Version 2    : Enabled
DSA Host Key Fingerprint : 48:4d:d0:97:0f:17:56:53:b1:23:6b:a1:5c:f2:9c:75
RSA Host Key Fingerprint : 6d:64:ad:db:23:49:23:37:11:65:20:6b:d5:6a:ea:0a
=====
SSH Server Router Instance [Base]
=====
Access allowed           : Allowed
-----
Connection               Username
  Version  Cipher      ServerName  Status
              MAC                      Key-re-exchange
-----
No entries found
=====
SSH Server Router Instance [management]
=====
Access allowed           : Allowed
-----
Connection               Username
  Version  Cipher      ServerName  Status
              MAC                      Key-re-exchange
-----
No entries found
=====
SSH Server Router Instance [1000]
=====
Access allowed           : Disallowed
-----
Connection               Username
  Version  Cipher      ServerName  Status
              MAC                      Key-re-exchange
-----
No entries found
=====
```

**Table 44 Show System Security SSH Detail Options Output Fields**

Label	Description
Administrative State	Enabled: The SSH server is enabled. Disabled: The SSH server is disabled.
Operational State	Up: The SSH server is up. Down: The SSH server is down.
Preserve Key	Enabled: The preserve-key is enabled. Disabled: The preserve-key is disabled.
Key-re-exchange	Displays the maximum time elapsed and the maximum number of Mbytes transmitted before a key re-exchange is initiated.
SSH protocol version 1	Enabled: SSH1 is enabled. Disabled: SSH1 is disabled.
SSH protocol version 2	Enabled: SSH2 is enabled. Disabled: SSH2 is disabled.
DSA Host 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 cannot continue with the SSH session since the server might be spoofed.
SSH Server Router Instance	SSH server router instance. Can be the router name ("Base" or "management") or the VPRN Id (1 to 2147483647).
Access Allowed	Allowed: Access to the SSH server is allowed. Disallowed: Access to the SSH server is disallowed.
Connection	The IP address of the connected routers (remote client).
Username	The name of the user.
Version	The SSH version number.

**Table 44 Show System Security SSH Detail Options Output Fields**

Label	Description (Continued)
Cipher	<p>3des: A SSHv1 encryption method that allows proprietary information to be transmitted over untrusted networks.</p> <p>3des-cbc: A SSHv2 encryption method.</p> <p>aes128-cbc: A SSHv2 128-bit encryption method.</p> <p>aes128-ctr: A SSHv2 128-bit encryption method.</p> <p>aes192-cbc: A SSHv2 192-bit encryption method.</p> <p>aes192-ctr: A SSHv2 192-bit encryption method.</p> <p>aes256-cbc: A SSHv2 256-bit encryption method.</p> <p>aes256-ctr: A SSHv2 256-bit encryption method.</p> <p>arcfour: A SSHv2 encryption method.</p> <p>des: A SSHv1 encryption method using a private (secret) key.</p> <p>blowfish: A SSHv1 encryption method.</p> <p>blowfish-cbc: A SSHv2 encryption method.</p> <p>cast128-cbc: A SSHv2 1280-bit encryption method.</p> <p>rijndael-cbc: A SSHv2 encryption method.</p>
Server Name	The server name.
Status	<p>connected: Displays that the SSH connection is connected.</p> <p>disconnected: Displays that the SSH connection is disconnected.</p>
MAC	<p>hmac-sha2-512: The SSH MAC algorithm used is hmac-sha2-512.</p> <p>hmac-sha2-256: The SSH MAC algorithm used is hmac-sha2-256.</p> <p>hmac-sha1: The SSH MAC algorithm used is hmac-sha1.</p> <p>hmac-sha1-96: The SSH MAC algorithm used is hmac-sha1-96.</p> <p>hmac-md5: The SSH MAC algorithm used is hmac-md5.</p> <p>hmac-ripemd160: The SSH MAC algorithm used is hmac-ripemd160.</p> <p>hmac-sha2-512: The SSH MAC algorithm used is hmac-sha2-512.</p> <p>hmac-ripemd160-openssh-com: The SSH MAC algorithm used is hmac-ripemd160-openssh-com.</p>
Key-re-exchange	Displays the maximum time elapsed and the maximum number of Mbytes transmitted before a key re-exchange is initiated for this session.
Number of SSH sessions	The total number of SSH sessions.

---

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**       The following is an example of user output information.

[Table 45](#) describes user output fields.

**Sample Output**

```
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
=====

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
```

```
=====
show system security user detail
=====
Users
=====
User ID      New User Permissions      Password Login   Failed Local
            Pwd console ftp li snmp netconf grpc Expires Attempt Logins Conf
-----
admin        n   y           y   n   y   y           n   never    9      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         : default
profile         : administrative
locked-out      : no
-----
snmp parameters
-----

show system security user logout
=====
Currently Failed Login Attempts
=====
User ID Remaining Login attempts Remaining Lockout Time (min:sec)
-----
jason123 N/A 9:56
-----
Number of users : 1
=====
```

**Table 45**      **Show System Security User Output Fields**

Label	Description
User ID	The name of a system user.
<b>Users</b>	
New Pwd	y — The user must change their password at the next login. n — The user does not need to change their password at the next login.



**Table 45 Show System Security User Output Fields (Continued)**

Label	Description (Continued)
User Permissions	<p>console:</p> <p>y — The user is authorized for console access.</p> <p>n — The user is not authorized for console access.</p> <p>ftp:</p> <p>y — The user is authorized for FTP access.</p> <p>n — The user is not authorized for FTP access.</p> <p>li:</p> <p>y — The user is authorized for LI access.</p> <p>n — The user is not authorized for LI access.</p> <p>snmp:</p> <p>y — The user is authorized for SNMP access.</p> <p>n — The user is not authorized for SNMP access.</p> <p>netconf:</p> <p>y — The user is authorized for NETCONF access.</p> <p>n — The user is not authorized for NETCONF access.</p> <p>grpc:</p> <p>y — The user is authorized for gRPC access.</p> <p>n — The user is not authorized for gRPC access.</p>
Password Expires	The number of days after which the user must change their password.
Login Attempt	The number of times that the user has attempted to log in, irrespective of whether the login succeeded or failed.
Failed Logins	The number of unsuccessful login attempts.
Local Conf	<p>y — Password authentication is based on the local password database.</p> <p>n — Password authentication is not based on the local password database.</p>
Number of users	The total number of listed users.
<b>User Configuration Detail</b>	
new pw required	<p>yes — The user must change their password at the next login.</p> <p>no — The user does not need to change their password at the next login.</p>
cannot change pw	<p>yes — The user does not have the ability to change their password.</p> <p>no — The user has the ability to change their password.</p>

**Table 45 Show System Security User Output Fields (Continued)**

Label	Description (Continued)
home directory	The local home directory for the user for both console and FTP access.
restricted to home	yes — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device. no — The user is allowed to navigate to a directory higher in the directory tree on the home directory device.
login exec file	The user's login exec file which executes whenever the user successfully logs in to a console session.
profile	The security profiles associated with the user.
locked-out	Whether the user is currently locked out, and, if they are locked out, how much time remains before the user can attempt to log into the node again.
<b>Currently Failed Login Attempts</b>	
Remaining Login Attempts	The number of login attempts remaining before the user is locked out.
Remaining Lockout Time (min:sec)	The number of minutes and seconds remaining until the lockout expires and the user can attempt to log in again.

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 46](#) shows the rules where pass and fail attempts are logged.

**Table 46 Pass/Fail Login Attempts**

Authentication Order	Client (such as, putty)	Server (such as, SR)		CLI Show System Security Attempts (SR)	
	Private Key Programmed	Public Key Configured	Password Configured	Logins Attempts	Failed Logins
1. Public Key	Yes	Yes	N/A	Increment	

**Table 46** Pass/Fail Login Attempts (Continued)

Authentication Order	Client (such as, putty)	Server (such as, SR)		CLI Show System Security Attempts (SR)	
	Private Key Programmed	Public Key Configured	Password Configured	Logins Attempts	Failed Logins
2. Password	Yes	Yes (No match between client and server. Go to password.)	Yes	Increment	
	Yes	No	Yes	Increment	
	No	N/A	Yes	Increment	
	No	N/A	No		Increment
1. Public Key (only)	Yes	Yes	N/A	Increment	
	Yes	Yes (No match between client and server. Go to password.)			Increment
	Yes		N/A		Increment
	No		N/A		Increment

## view

**Syntax** **view** [*view-name*] [**detail**]

**Context** show>system>security

**Description** This command displays the SNMP MIB views.

**Parameters** *view-name* — Specifies 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** The following is an example of SNMP MIB view information.

[Table 47](#) describes show view output fields.

### Sample Output

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

view name	oid tree	mask	permission
iso	1		included
read1	1.1.1.1	11111111	included
writel	2.2.2.2	11111111	included
testview	1	11111111	included
testview	1.3.6.1.2	11111111	excluded
mgmt-view	1.3.6.1.2.1.2		included
mgmt-view	1.3.6.1.2.1.4		included
mgmt-view	1.3.6.1.2.1.5		included
mgmt-view	1.3.6.1.2.1.6		included
mgmt-view	1.3.6.1.2.1.7		included
mgmt-view	1.3.6.1.2.1.31		included
mgmt-view	1.3.6.1.2.1.77		included
mgmt-view	1.3.6.1.4.1.6527.3.1.2.3.7		included
mgmt-view	1.3.6.1.4.1.6527.3.1.2.3.11		included
vprn-view	1.3.6.1.2.1.2		included
vprn-view	1.3.6.1.2.1.4		included
vprn-view	1.3.6.1.2.1.5		included
vprn-view	1.3.6.1.2.1.6		included
vprn-view	1.3.6.1.2.1.7		included
vprn-view	1.3.6.1.2.1.15		included
vprn-view	1.3.6.1.2.1.23		included
vprn-view	1.3.6.1.2.1.31		included
vprn-view	1.3.6.1.2.1.68		included
vprn-view	1.3.6.1.2.1.77		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.3.7		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.3.11		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.20.1		included
no-security	1		included
no-security	1.3.6.1.6.3		excluded
no-security	1.3.6.1.6.3.10.2.1		included
no-security	1.3.6.1.6.3.11.2.1		included
no-security	1.3.6.1.6.3.15.1.1		included
on-security	2	00000000	included

No. of Views: 33

=====

A:ALA-48#

**Table 47** 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.

## certificate

<b>Syntax</b>	<b>certificate</b>
<b>Context</b>	show
<b>Description</b>	This command displays certificate information.

## ca-profile

<b>Syntax</b>	<b>ca-profile</b> <b>ca-profile</b> <i>name</i> [ <b>association</b> ]
<b>Context</b>	show>certificate
<b>Description</b>	This command shows certificate-authority profile information.
<b>Parameters</b>	<i>name</i> — Specifies the name of the Certificate Authority (CA) profile. <b>association</b> — 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>	This command displays the current cached OCSP results. The output includes the following information:  Certificate issuer  Certificate serial number  OCSP result  Cache entry expire time
<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.

## 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.
<b>Output</b>	<a href="#">Table 48</a> describes Distributed CPU Protection output fields.

**Table 48 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 XCM can house multiple FPs via its two XMA's).
Dynamic Enforcement Policer Pool	The configured size of the dynamic-enforcement-policer-pool for this card or 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 ( <b>clear card x fp y dist-cpu-protection</b> )
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.

### Sample Output

```
*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
-----
=====
```

**Table 49** 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 XCM can house multiple FPs via its two XMA's).
Dynamic Enforcement Policer Pool	The configured size of the dynamic-enforcement-policer-pool for this card or 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 ( <b>clear card x fp y dist-cpu-protection</b> )
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.

## 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> — Specifies to 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 kb/s, and so on, are displayed.

**Output** Distributed CPU Protection Policer Output

[Table 50](#) describes Distributed CPU Protection Policer output fields.

**Table 50** 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 XCM can house multiple FPs via its two XMA's).
Policer-State	The state of the policer with the following potential values:
	Exceed - The policer has been detected as not conforming to the associated DCP policy parameters (for example, packets exceeded the configured rate and the DCP polling process identified this occurrence)
	Conform - The policer has been detected as conforming to the associated DCP policy parameters (rate)
	not-applicable - Newly-created policers or policers that are not currently instantiated. This includes policers configured on line cards that are not in service.
Protocols Mapped	A list of protocols that are configured to map to the particular policer.



**Table 50 Show Distributed CPU Protection Policer Output Fields**

Label	Description
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 <b>detail</b> keyword is included in the show command. 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 kb/s, and so on, are displayed.</p> <p>Oper. Kbps - The adapted “kilobits-per-second” value for DCP “kbps” rates</p> <p>Oper. MBS - The adapted “mbs size” value for DCP “kbps” rates</p> <p>Oper. Depth - The calculated policer bucket depth in packets (for DCP “packets” rates) or in bytes (for DCP “kbps” rates)</p> <p>Oper. Packets - The adapted “ppi” value for DCP “packets” rates</p> <p>Oper. Within - The adapted “within seconds” value for DCP “packets” rates</p> <p>Oper. Init. Delay - 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 conforming 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 conforming.
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 conforms again.
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                      Policer-State      : Conform
Protocols Mapped  : arp
Exceed-Count      : 0
Detec. Time Remain : 0 seconds                Hold-Down Remain.  : none
Operational (adapted) rate parameters:
  Oper. Packets    : 5 ppi                      Oper. Within       : 8 seconds
  Oper. Initial Delay: 6 packets
  Oper. Depth      : 0 packets

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

... (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                      Policer-State      : conform
Protocols Mapped  : arp, pppoe-pppoa
Exceed-Count      : 0
All Dyn-Plcr Alloc. : False
Operational (adapted) rate parameters:
  Oper. Packets    : 10 ppi                      Oper. Within       : 8 seconds
  Oper. Initial Delay: 8 packets
  Oper. Depth      : 0 packets
-----

```

```

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

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

```

## dist-cpu-protection

- Syntax** **dist-cpu-protection [detail]**
- Context** show>router>interface
- Description** This command displays Distributed CPU Protection parameters and status at the router Interface level.
- Parameters** **detail** — Specifies to 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 kb/s, and so on, are displayed.
- Output** Distributed CPU Protection Policer Output

[Table 51](#) describes Distributed CPU Protection Policer output fields.

**Table 51 Show Distributed CPU Protection Policer Output Fields**

Label	Description
Distributed CPU Protection Policy	Displays the DCP policy assigned to the object.
Policer-Name	Displays the configured name of the static policer
Card/FP	Displays 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 XCM can house multiple FPs via its two XMAS).

**Table 51 Show Distributed CPU Protection Policer Output Fields**

Label	Description
Policer-State	Displays the state of the policer with the following potential values:
	<i>Exceed</i> - The policer has been detected as nonconforming to the associated DCP policy parameters (packets exceeded the configured rate and the DCP polling process identified this occurrence)
	<i>Conform</i> - The policer has been detected as conforming to the associated DCP policy parameters (rate)
	<i>not-applicable</i> - newly-created policers or policers that are not currently instantiated. This includes policers configured on line cards that are not in service.
Protocols Mapped	Displays 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 <b>detail</b> keyword is included in the show command. 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 kb/s, and so on, are displayed.</p> <p><i>Oper. Kbps</i> - Displays the adapted “kilobits-per-second” value for DCP “kbps” rates</p> <p><i>Oper. MBS</i> - Displays the adapted “mbs size” value for DCP “kbps” rates</p> <p><i>Oper. Depth</i> - Displays the calculated policer bucket depth in packets (for DCP “packets” rates) or in bytes (for DCP “kbps” rates)</p> <p><i>Oper. Packets</i> - Displays the adapted “ppi” value for DCP “packets” rates</p> <p><i>Oper. Within</i> - Displays the adapted “within seconds” value for DCP “packets” rates</p> <p><i>Oper. Init. Delay</i> - Displays the adapted “initial-delay packets” value for DCP “packets” rates</p>

**Table 51 Show Distributed CPU Protection Policer Output Fields**

Label	Description
Exceed-Count	Displays the count of packets exceeding the policing parameters since the given policer was previously declared as conforming 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 conforming.
Detec. Time Remain	Displays the remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it conforms again.
Hold-Down Remain	Displays 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
-----
=====

```

**Table 52 Show Distributed CPU Protection Policer Output Fields**

Label	Description
Distributed CPU Protection Policy	Displays the DCP policy assigned to the object.
Policer-Name	Displays the configured name of the static policer
Card/FP	Displays 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 XCM can house multiple FPs via its two XMA's).
Policer-State	Displays the state of the policer with the following potential values:  Exceed — The policer has been detected as nonconforming to the associated DCP policy parameters (packets exceeded the configured rate and the DCP polling process identified this occurrence).  Conform — The policer has been detected as conforming to the associated DCP policy parameters (rate).  not-applicable — Newly-created policers or policers that are not currently instantiated. This includes policers configured on linecards that are not in service.
Protocols Mapped	Displays a list of protocols that are configured to map to the particular policer.

**Table 52 Show Distributed CPU Protection Policer Output Fields**

Label	Description
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 <b>detail</b> keyword is included in the show command. 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 kb/s, and so on, are displayed.</p> <p>Oper. Kbps — Displays the adapted “kilobits-per-second” value for DCP “kbps” rates</p> <p>Oper. MBS — Displays the adapted “mbs size” value for DCP “kbps” rates</p> <p>Oper. Depth — Displays the calculated policer bucket depth in packets (for DCP “packets” rates) or in bytes (for DCP “kbps” rates)</p> <p>Oper. Packets — Displays the adapted “ppi” value for DCP “packets” rates</p> <p>Oper. Within — Displays the adapted “within seconds” value for DCP “packets” rates</p> <p>Oper. Init. Delay — Displays the adapted “initial-delay packets” value for DCP “packets” rates</p>
Exceed-Count	Displays the count of packets exceeding the policing parameters since the given policer was previously declared as conforming 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 conforming.
Detec. Time Remain	Displays the remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it conforms again.
Hold-Down Remain	Displays 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.

2.9.2.1.3 Login Control

users

- Syntax** users
- Context** show
- Description** Displays console user login and connection information.
- Output** The following is an example of user information.

Table 53 describes show users output fields.

Sample Console Users Output

```
*A:node-1# show users
=====
User
  Session ID  From                Type      Login time      Idle time
=====
      6              --                Console      --              3d 10:11:02 --
admin
  83            192.168.255.255    SSHv2      12OCT2018 20:44:15  0d 00:00:50 A-
admin
  #84           192.168.255.255    SSHv2      12OCT2018 21:09:25  0d 00:00:00 --
-----
Number of users: 2
'#' indicates the current active session
'A' indicates user is in admin mode
=====
```

Table 53 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.



---

## 2.9.2.2 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, and so on), the entire string must be enclosed within double quotes. <i>ip-address</i> — Clears the authentication statistics for the specified IP address.

### 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. <b>statistics</b> — Clears statistics for the specified server.

### 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>	<i>entry-id</i> — Specifies a particular CPM IP filter entry. <b>Values</b> 1 to 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 information and only applies to the 7750 SR and 7950 XRS.

---

**Parameters**    *entry-id* — Specifies a particular CPM IPv6 filter entry.  
**Values**        1 to 2048

## ipv6-filter

**Syntax**        **ipv6-filter** [**entry** *entry-id*]  
**Context**        clear>cpm-filter  
**Description**    This command clears IPv6 filter statistics.  
**Parameters**    *entry-id* — Specifies a particular CPM IP filter entry.  
**Values**        1 to 2048

## mac-filter

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

### 2.9.2.2.1 CPU Protection Commands

## cpu-protection

**Syntax**        **cpu-protection**  
**Context**        clear  
**Description**    This command enables the context to clear CPU protection data.

## excessive-sources

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

---

## protocol-protection

<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. <b>interface</b> — Clears entries for interfaces. <b>sap</b> — Clears entries for SAPs.

## cpm-queue

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

### 2.9.2.3 Debug Commands

## radius

<b>Syntax</b>	<b>radius [detail] [hex] no radius</b>
<b>Context</b>	debug
<b>Description</b>	This command enables debugging for RADIUS connections.  The <b>no</b> form of the command disables the debug output.

---

**Parameters**    **detail** — Displays detailed output.  
                  **hex** — Displays the packet dump in hex format.

## certificate

**Syntax**        **certificate**  
**Context**       **debug**  
**Description**   This command enters the debug certificate context.

## ocsp

**Syntax**        **[no] ocsp**  
**Context**       **debug>certificate**  
**Description**   This command enables debug output of the OCSP protocol for a CA profile.  
                  The **no** form of this command disables the debug output.

## ca-profile

**Syntax**        **[no] ca-profile** *profile-name*  
**Context**       **debug>certificate>ocsp**  
**Description**   This command enables debug output for a specific CA profile.  
                  The **no** form of this command disables the debug output.  
**Parameters**   *profile-name* — Specifies the profile name, up to 32 characters.

## grpc

**Syntax**        **[no] grpc**  
**Context**       **debug>system**  
**Description**   This command enables the debug context for gRPC.  
                  The **no** form of this command removes any debug activation within the gRPC context.

## client

<b>Syntax</b>	<b>client all</b> <b>client <i>ip-address</i></b> <b>no client</b>
<b>Context</b>	debug>system>grpc
<b>Description</b>	This command enables debug output for all clients for a particular client.  The <b>no</b> form of this command deactivates debugging for all clients.
<b>Parameters</b>	<b>all</b> — Specifies that debugging will occur for all clients.  <i>ip-address</i> — Specifies the IPv4 or IPv6 address of the client.

## type

<b>Syntax</b>	<b>type all</b> <b>type [gnmi-capabilities] [gnmi-get] [gnmi-set] [gnmi-subscribe]</b> <b>no type</b>
<b>Context</b>	debug>system>grpc
<b>Description</b>	This command enables debugging for all RPCs or a particular RPC.  The <b>no</b> form of this command deactivates debugging for all RPCs.
<b>Parameters</b>	<b>all</b> — Specifies that debugging is enabled for all RPCs.  <b>gnmi-capabilities</b> — Specifies that debugging is enabled for gNMI capability RPC. <b>gnmi-get</b> — Specifies that debugging is enabled for gNMI get RPC. <b>gnmi-set</b> — Specifies that debugging is enabled for gNMI set RPC. <b>gnmi-subscribe</b> — Specifies that debugging is enabled for gNMI subscribe RPC.

### 2.9.2.4 Tools Commands

## dist-cpu-protection

<b>Syntax</b>	<b>dist-cpu-protection</b>
<b>Context</b>	tools>perform>security tools>dump>security

**Description** This command displays to release Distributed CPU Protection parameters and status at the per card and forwarding plane level.

## violators

**Syntax** **violators enforcement** {**sap** | **interface**} **card** *slot-number* [**fp** *fp-number*]  
**violators local-monitor** {**sap** | **interface**} **card** *slot-number* [**fp** *fp-number*]

**Context** tools>dump>security>dist-cpu-protection

**Description** This command shows the nonconforming enforcement policers and local monitors.

**Parameters** **sap** — -Indicates to display the violators associated with SAPs  
**interface** — - Indicates to display the violators associated with router interfaces.  
**enforcement** — Shows exceed and hold-down for Static and Dynamic Policers.  
**local-monitor** — Shows state of dynamic policer allocation for Local Monitoring Policers.  
**card** *slot-number* — The physical slot number for the card.

**Values** 1 to n (n is platform dependent)

**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 XCM can house multiple FPs via its two XMAAs).

**Values** 1 to 8

**Output** Users Output

[Table 54](#) describes show users output fields.

**Table 54** 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
=====
```

## 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> ] <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-cpu-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. <b>sap</b> <i>sap-id</i> — Specifies sap identifier. <b>protocol</b> <i>protocol</i> — Specifies DCP protocol name (for example, arp, dhcp) <b>static-policer</b> <i>name</i> — Specifies DCP static policer name as defined in the DCP policy.

## 2.9.2.5 Admin Commands

### logout

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

---

## password-history

<b>Syntax</b>	<b>password-history</b> { <b>user</b> <i>user-name</i>   <b>all</b> }
<b>Context</b>	admin>clear
<b>Description</b>	This command is used to clear old passwords used by a specific user, or for all users.
<b>Parameters</b>	<i>user-name</i> — Clears the password history information about the specified user, up to 32 characters. <b>all</b> — Clears the password history information for all users.



## 3 Classic and Model-Driven Management Interfaces

SR OS supports two basic classes of management interfaces:

- classic management interfaces
- model-driven management interfaces

Classic management interfaces include:

- SNMP
- the classic CLI
- NETCONF using the Alcatel-Lucent Base-R13 SR OS YANG modules

Model-driven management interfaces include:

- the MD-CLI
- NETCONF using the Nokia SR OS YANG modules
- the gRPC Network Management Interface (gNMI)

References to the term “CLI” in the SR OS user documentation are generally referring to the classic CLI. The classic CLI is the CLI that has been supported in SR OS from the initial introduction of SR OS.

The MD-CLI is a model-driven CLI introduced in SR OS Release 16.0.R1. Refer to *The MD-CLI User Guide* and *The MD-CLI Command Reference Guide* for details on using configuration commands in the MD-CLI.

### 3.1 Model-Driven Management Interfaces

Model-driven management interfaces are based on a common infrastructure that uses YANG models as the core definition for configuration, state, and operational actions. All model-driven interfaces take the same common underlying YANG modules and render them for the particular management interface.

The Nokia SR OS YANG modules of the model-driven infrastructure are similar to the classic CLI tree with the following notable differences:

- the classic and model-driven configuration formats are incompatible; the system automatically converts the classic configuration to model-driven format when the management interface configuration mode is changed to **model-driven**

- some classic CLI branches have been moved, renamed, or re-organized in the SR OS YANG modules
- many elements use string names as keys in model-driven interfaces instead of the numerical identifiers used in the classic CLI and SNMP. The name can only be assigned or modified for these elements in releases prior to Release 15.1.R1. Elements without names are automatically assigned a name (the identifier converted to a string) during an upgrade to Release 15.1.R1 or later, and cannot be changed without manually deleting and recreating the element. It is recommended that the following elements are assigned names prior to an upgrade to Release 15.1 or later:
  - all services (**configure service vprn**, **vpls**, **epipe**, and so on)
  - **configure mirror mirror-dest**
  - **configure service pw-templates**
  - **configure service customer**
  - **configure filter ip-filter**, **ipv6-filter**, and **mac-filter**
  - **configure qos network**, **sap-ingress**, and **sap-egress**
  - **configure eth-cfm domain** and **association**
- the classic CLI **shutdown** command has been replaced with **admin-state** in model-driven interfaces
- the classic CLI commands with multiple parameters have been separated into individual leaves in model-driven interfaces
- the model-driven interfaces make extensive use of Boolean values (true and false) for configuration settings

In model-driven configuration-mode, SR OS operates with 'explicit' default handling. Users can set a leaf to the same value as the default, and SR OS remembers that it was explicitly set, and displays it as part of the configuration. This is similar to what RFC6243 refers to as 'explicit' mode.

In the classic configuration-mode, the default handling is similar to RFC6243 'trim' mode. Configuration values are not reported if they are equal to the default value, even if the user explicitly configured the value.

In mixed configuration-mode, the system uses 'explicit' default handling but it is not persistent. Explicitly configured default values are lost or forgotten at a High-availability CPM switchover or a reboot. Nokia does not recommend setting any leaf explicitly to its default value in mixed configuration-mode (the leaf should be deleted instead).

---

### 3.1.1 Prerequisites for Using Model-Driven Management Interfaces

Before configuration editing is permitted in model-driven interfaces, the management interface configuration mode must be set to **model-driven** or **mixed**. Refer to [Management Interface Configuration Mode](#) for details.

All loose references using IDs to certain elements (elements which use IDs as keys in classic interfaces but string names in model-driven interfaces) must be replaced with references using string names. Refer to [Loose References to IDs](#) for details.

Strict routing policy validation is used for model-driven interfaces. The routing policy must exist for the management interface configuration mode to be changed. References to non-existent routing policies must be removed before attempting to switch modes. Strict policy validation is applied to the following routing policy references:

- BGP: in the Base router and VPRN instances
- IS-IS: in the Base router and VPRN instances
- LDP
- OSPF and OSPFv3: the Base router and VPRN instances
- Policy-option: **from**, **to**, **action**, and **default-action** statements
- Policy-option: sub-policies, **prefix-list**, **as-path**, **as-path-group**, **damping**, and **community** policies
- RIP and RIPng: in the Base router and VPRN instances
- Single policy-statement or logical policy expressions
- VPLS: for BGP VSI
- VPRN: for GRT, MVPN, and VRF

## 3.2 YANG Data Models

Model-driven management interfaces are based on a common infrastructure that uses YANG models as the core definition for configuration, state, and operational actions. All model-driven interfaces take the same common underlying YANG modules and render them for the particular management interface.

The SR OS supports:

- SR OS YANG data models
- OpenConfig YANG data models

### 3.2.1 SR OS YANG Data Models

The SR OS supports two similar proprietary YANG configuration data models. A unique set of XML namespaces is used for each of the two data models.

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

- The names of the modules are `alu-conf-r13` (for example, `alu-conf-log-r13`). Note the `-r13` suffix at the end of the names.
- The Alcatel-Lucent Base-R13 model consists of a set of modules with groupings that are all used by a single top-level configuration module called `alu-conf-r13`. All configuration data in the Alcatel-Lucent Base-R13 models sits in the `urn:alcatel-lucent.com:sros:ns:yang:conf-r13` XML namespace.
- The Base-R13 modules can only be used in the NETCONF interface and only with the `<running>` datastore. They can not be used with the NETCONF `<candidate>` datastore or with any other management interface.
- Although the Base-R13 modules were first introduced in SR OS Release 13.0, they do not only contain objects from Release 13.0. For example, features from any later release are also configurable using versions of the Base-R13 modules that are distributed with that release.
- The Base-R13 modules align closely to the structure and behavior of the SR OS classic CLI.

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

- The names of the modules and submodules are `nokia-conf-*` (for example, `nokia-conf-log`). They have no `-r13` suffix in the names.

- The Nokia SR OS YANG configuration model is divided into a single top-level configuration module (nokia-conf), a set of submodules (for example, nokia-conf-system), and a set of nokia-types-\* modules. All configuration data in the Nokia SR OS YANG models sit in the urn:nokia.com:sros:ns:yang:sr:conf XML namespace. All state data in the Nokia SR OS YANG models sits in the urn:nokia.com:sros:ns:yang:sr:state XML namespace.
- The modules can be used with NETCONF with the <candidate> or <running> datastores, with telemetry, or with the Set/Get RPCs of the gRPC-based gNMI service. The modules map to the MD-CLI interface.
- The modules and submodules indicate the SR OS major release stream using a YANG extension (for example, sros-ext:sros-major-release "rel16";). Module and submodule revisions form a contiguous series of revisions inside a major release stream. There may be two files for the same module with the same revision date but with different contents because they are from two different major release streams. Each active major release stream has revisions ongoing in parallel.
- An alternative packaging of the entire Nokia configuration model is available in the single file called nokia-conf-combined.yang.

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

There is a single YANG state model for SR OS with the following attributes.

- The names of the modules and submodules are nokia-state-\* (for example, nokia-state-log).
- The Nokia SR OS YANG state model is divided into a single top-level statistics module (nokia-state), a set of submodules (for example, nokia-state-system), and a set of nokia-types-\* modules. All state data in the Nokia SR OS YANG models sits in the urn:nokia.com:sros:ns:yang:sr:state XML namespace.
- The modules can be used with NETCONF or telemetry.
- An alternative packaging of the entire state model is available in the single file called nokia-state-combined.yang.

All configuration modules, state modules, and **types** modules are advertised in the SR OS NETCONF server <hello>. Submodules are not advertised in the <hello>.

The **bof**, **admin**, **tools**, **debug**, or **clear** branches of the CLI do not have equivalent YANG data models.

## 3.2.2 OpenConfig YANG Data Models

OpenConfig presents a vendor-independent set of YANG models. OpenConfig YANG model attributes are mapped to application-specific configuration and state. SR OS requires the following system management configuration to access the application configuration using the OpenConfig YANG models.

```
(ex) [configure system management-interface]
configuration-mode model-driven
cli {
    cli-engine [md-cli]
}
yang-modules {
    openconfig-modules true
}
```

OpenConfig YANG models are available for all model-driven interfaces. In MD-CLI, OpenConfig configuration is located in the **configure openconfig** context.

When a configuration is committed, the system checks to ensure that **openconfig-modules** is set to **true**. If **openconfig-modules** is set to **false**, a configuration error is raised.

The **openconfig-modules** command behaves differently depending on the configuration access method, MD-CLI, gNMI, or NETCONF as follows:

- Using the MD-CLI interface, users can configure and execute OpenConfig configuration edits.
  - During the interactive configuration of OpenConfig commands, only OpenConfig syntax is checked.
  - When a configuration is committed, the system verifies that **openconfig-modules** is set to true. If **openconfig-modules** is not set to **true** and there are OpenConfig configuration transactions, the commit fails.
  - The operator must set **openconfig-modules** to **true** and perform the **commit** again. Assuming the configuration information is complete and there are no other errors, the transaction succeeds.
- For the gNMI and NETCONF interfaces, **openconfig-module** is checked to determine if OpenConfig models are being advertised and if the system can accept or send OpenConfig model configurations, states, or requests.
  - If the OpenConfig modules are not enabled, then the sending and accepting of OpenConfig edits, requests, and responses is blocked at the gNMI or NETCONF level.
  - A 'get' from the root without any declared namespace or branch succeeds but does not include any OpenConfig data. However, a 'get' that explicitly requests data from the OpenConfig namespace produces an error.

It is possible to configure the network element using both Nokia YANG and OpenConfig YANG models. Configuration ownership is a key concept, determining which model-driven access method can update a container or list entry. Only the access method that has claimed configuration ownership of an container or list entry can modify the configuration for that container or list entry. Individual applications define the required container or list entry based on their unique requirements. The applications also determines if and how ownership can change. It is possible to have both Nokia YANG and OpenConfig YANG commands in the same set transaction. Validation and commit functions apply to all transactions in a single set. If an access method attempts to configure elements under a part of the hierarchy it does not own, an error message is generated. An example of the error message is:

```
MINOR: MGMT_CORE #261: configure openconfig interfaces interface "1/1/1" -  
Cannot access or modify element - managed by Nokia module
```

Configuration ownership also influences default imports. The owner imports their container or list entry defaults. In the case where OpenConfig is the container or list entry owner but the model has opted to omit configuration elements required for application functionality, the Nokia application defaults are imported. These defaults cannot be modified using OpenConfig if the configuration path is not included in the OpenConfig model. If an object in the OpenConfig model does not specify a default, the application can use any default available. Typically, this is the existing SR OS application default for the container or list entry.

In the case where the OpenConfig model includes a leaf but does not include a default, the Nokia default can be used as specified in [Table 55](#).

**Table 55**      **Default Behavior**

Case	OpenConfig leaf value specified	OpenConfig leaf has YANG default	Action taken
1	yes	yes	Use OC leaf value specified
2	yes	no	Use OC leaf value specified
3	no	yes	Use OC leaf default value
4	no	no	Use Nokia default value

An operator action, such as the modification of a container or list entry using OpenConfig, may transition the container or list entry ownership to OpenConfig. Transitioning from OpenConfig to Nokia configuration ownership usually requires the deletion of the container or list entry through the OpenConfig model.

If the Nokia models are to be considered for configuration, the **nokia-modules** or **nokia-combined-modules** parameter must be set to **true** in the **configure system management-interface yang-modules** context.

When model-driven management interface configuration mode and OpenConfig YANG are enabled, the OpenConfig YANG configuration options become available. The **openconfig-modules true** command can be changed to **openconfig-modules false** during operation. However, all OpenConfig YANG configuration statements must be deleted prior to deleting the **openconfig-modules** leaf or setting it to **openconfig-modules false**, otherwise an error is generated. This protects the system from entering a state where an OpenConfig mismatch is possible.

The **validate** command validates the model-driven configuration against the model-specific definition, including any deviations. The **commit** command performs application-level mappings, another validation function, and activation of the candidate datastore. The application-specific mapping ensures the application requirements are met using the same criteria that is common for that application across all configuration actions.

In cases where there is an incomplete set of modeled data which results in an error, or there are other errors that arise from the commit operation, all transactions fail and produce an error message indicating the reason for the failure. A failure maintains the complete set of YANG parameters, as if the **commit** command had not been issued. This allows the administrator the option to correct the source of the error. Partial configurations are allowed as determined by the application and are not themselves invalid.

The transaction is tracked, including the OpenConfig Key and the Nokia Key. Both the OpenConfig path and the Nokia path are included in the returned error message. This error message uses the following format; Nokia:Normalized:OC-Key/path. This approach allows error message parsing and extraction of preference for the operator's model-driven-specific approach. A sample error message is shown below.

```
<severity>: <module> #<code>: <context in which the error occurred> - <message> -  
<extra-text> - <extra-context>
```

where <extra-context> could be the OpenConfig context or related key information.

Deviation files are available for each model where there are differences from the published OpenConfig model. These deviations can include not-supported, add, replace, granularity mismatches, and different ranges. The OpenConfig YANG file contains text descriptions when different units or ranges are in place. Deviations are not raised for OpenConfig “must” statements as the “must” statement in OpenConfig models is not supported in SR OS. The deviation file follows this format **nokia-sr-*<ocmodule>*-deviations.yang**, for example, **nokia-sr-openconfig-network-instance-deviations.yang**.



There are several places where ranges and units may not be aligned between OpenConfig YANG and SR OS application implementation.

When a mapping exists for an attribute but the configuration is out of range, an error is generated. For example, the application configuration leafB has a range of (1..100), where OpenConfig leafB specifies a range of (1...300). When an OpenConfig set above 100 is requested, an unsupported value error is returned.

As an example of a granularity mismatch, application leafC supports centiseconds and OpenConfig leafC supports milliseconds. If the OpenConfig value in milliseconds can be converted to a valid application value, the OpenConfig value is accepted (for example, OpenConfig leafC 100 ms is converted to application leafC 1 centisecond). However, if the OpenConfig value cannot be converted to a valid application value, an error is produced (for example, OpenConfig leafC 125ms cannot be mapped into centiseconds).

### 3.3 System-Provisioned Configuration (SPC) Objects

There is a set of configuration objects (configuration list elements and their descendants) that are provisioned (added to the <running> datastore) automatically by SR OS; for example, log-id 99. Some SPC objects are created at bootup time, and some are created or removed dynamically based on configuration. The dynamically created SPC objects are typically children objects created as a side effect of the creation of their parent object.

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

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

```
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 ssh client-cipher-list protocol-version 1 cipher 200-210
Config system security ssh client-cipher-list protocol-version 2 cipher 190-235
Config system security ssh server-cipher-list protocol-version 1 cipher 200-205
Config system security ssh server-cipher-list protocol-version 2 cipher 190-235
Config log filter 1001
Config log filter 1001 entry 10
Config log log-id 99 & 100
```

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

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

```
Config system security user-template {tacplus_default|radius_default}
Config system security snmp view iso ...
Config system security snmp view li-view ...
Config system security snmp view mgmt-view ...
Config system security snmp view vprn-view ...
Config system security snmp view no-security-view ...
Config system security snmp access group xyz (a set of access groups)
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"
Config eth-cfm default-domain bridge-identifier <x>
```

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

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

## 3.4 Management Interface Configuration Mode

Management interface configuration mode controls how classic management interfaces, such as SNMP and the classic CLI, and model-driven (MD) interfaces, such as the MD-CLI and NETCONF, are used to modify the configuration of the router. The **configure system management-interface configuration-mode** command must be used to enable configuration editing by MD interfaces.

**Table 56 Management Interface Configuration Mode**

		Configuration Mode		
		Classic	Mixed	Model-driven
Classic Interfaces	Classic CLI: configuration write/edit	OK	OK	—
	Classic CLI: configuration read	OK	OK	OK
	Classic CLI: non-configuration commands	OK	OK	OK
	SNMP: configuration write/edit	OK	OK	—
	SNMP: non-configuration writes (such as admin reboot)	OK	OK	—
	SNMP: configuration read	OK	OK	OK
	SNMP: state read	OK	OK	OK
	SNMP: notifications (traps)	OK	OK	OK
	NETCONF (Base-R13 model): configuration write/edit	OK	OK	—
	NETCONF (Base-R13 model): configuration read	OK	OK	OK
Model-driven Interfaces	NETCONF (Nokia model): configuration write and read	—	OK	OK
	NETCONF (Nokia model): state read	OK	OK	OK
	Telemetry: configuration nodes	—	OK	OK
	Telemetry: state nodes	OK	OK	OK
	gNMI Set/Get: configuration write and read	—	OK	OK
	gNMI Get: state read	OK	OK	OK

**Table 56** Management Interface Configuration Mode (Continued)

		Configuration Mode		
		Classic	Mixed	Model-driven
Features	OpenConfig YANG models	—	—	OK
	Configuration Groups	—	—	OK
	MD-CLI <b>rollback</b> command	—	—	OK
	Classic CLI <b>admin rollback revert</b> command	OK	OK	—
	Explicit defaults <sup>1</sup>	—	—	OK
	Configuration changes accepted immediately after a CPM high-availability switchover <sup>2</sup>	OK	—	OK

Note:

1. In **model-driven** mode, users can set a leaf to the same value as the default, and SR OS remembers that it was explicitly set and displays it as part of the configuration. In mixed mode these values are not persistent and they are lost or forgotten at a CPM high-availability switchover or a reboot.
2. In **mixed** configuration-mode, changes to configuration are blocked for a few minutes after a CPM high-availability switchover event while the model-driven database is synchronized with the application layer of SR OS. There is no impact to running services.

### 3.4.1 Mixed Configuration Mode

Mixed configuration mode is useful for operators to migrate from classic management interfaces to operating in a full model-driven mode. It allows the use of previous classic CLI scripts or other OSS integration (for configuration) although with some pre-requisites (see [Prerequisites for Using Model-Driven Management Interfaces](#)) and some limitations (see [Table 56](#)).

## 3.4.2 Loose References to IDs

A loose reference is a reference where the target of the reference does not have to exist. For example, **configure service pw-template 23 egress filter ip 37** can be configured (when the management interface configuration mode is **classic**) even if **ip-filter 37** does not yet exist in the configuration.

Before switching the management interface configuration mode to **model-driven** or **mixed**, all loose references using IDs must be replaced with references using string names (or removed from the configuration) for the following elements:

- all services (**configure service vprn**, **vpls**, **epipe**, and so on)
- **configure mirror mirror-dest**
- **configure service pw-templates**
- **configure service customer**
- **configure filter ip-filter**, **ipv6-filter**, and **mac-filter**
- **configure qos network**, **sap-ingress**, and **sap-egress**
- **configure eth-cfm domain** and **association**

In the following configuration example,

```
configure service pw-template 23 egress filter ip 37
```

can be changed to

```
configure service pw-template 23 egress filter-name ip ops-sec-filter-a33
```

Because **ip-filter 37** is a loose reference, it does not require a name for the configuration to be valid. However, it may be desirable to assign a name as follows, to make the binding operational.

```
configure filter ip-filter 37 name ops-sec-filter-a33
```



**Note:** A name can only be assigned to a filter or any element in the above list of elements which use IDs as keys in classic interfaces but string names in model-driven interfaces. It is recommended to assign names to the elements prior to an upgrade to Release 15.1.R1.

A name can also be changed in releases prior to Release 15.1.R1. Elements without names are automatically assigned a name (the ID converted to a string) during an upgrade to Release 15.1.R1 or later, and cannot be changed without manually deleting and recreating the element.

Loose references to IDs for the objects listed above cannot be created while in **mixed** or **model-driven** configuration mode. Any classic CLI scripts must also be updated to avoid the use of any of the commands below.

The following lists the set of affected loose references. Some items take a service-name as an input. SR OS converts these service-names to IDs, and stores the IDs in the configuration. In these cases, the service-name becomes an alias at configuration edit time and is not stored as a reference.

#### IPSec related configuration:

```
configure service vprn interface sap ipsec-tunnel local-gateway-address
configure service vprn interface sap ip-tunnel delivery-service
configure service vprn interface sap l2tpv3-session router
configure service epipe sap l2tpv3-session router
configure service vpls sap l2tpv3-session router
configure service vprn interface sap ipsec-gw default-secure-service
configure service ies interface sap ipsec-gw default-secure-service
configure service vprn interface sap ipsec-gw dhcp server
configure service ies interface sap ipsec-gw dhcp server
configure service vprn interface sap ipsec-gw dhcp6 server
configure service ies interface sap ipsec-gw dhcp6 server
configure service vprn interface sap ipsec-gw local-address-assignment ipv4 address-
source
configure service vprn interface sap ipsec-gw local-address-assignment ipv6 address-
source
configure service ies interface sap ipsec-gw local-address-assignment ipv4 address-
source
configure service ies interface sap ipsec-gw local-address-assignment ipv6 address-
source
configure service vprn interface sap ipsec-tunnel bfd-enable
configure ipsec client-db client private-service
configure system file-transmission-profile router
```

#### Eth-cfm, oam-pm, and saa:

```
configure eth-cfm default-domain bridge-identifier
configure eth-cfm domain association bridge-identifier
configure oam-pm session ip router
configure oam-pm session ip router service-name
configure saa test type cpe-ping service
configure saa test type icmp-ping router
configure saa test type icmp-ping service-name
configure saa test type icmp-trace router
configure saa test type icmp-trace service-name
configure saa test type mac-ping service
configure saa test type mac-trace service
configure saa test type vprn-ping
configure saa test type vprn-ping service
configure saa test type vprn-trace
configure saa test type vprn-trace service
```

#### Filters:

```
configure service pw-template egress filter ipv6
```

```
configure service pw-template egress filter ip
configure service pw-template egress filter mac
configure service pw-template ingress filter ipv6
configure service pw-template ingress filter ip
configure service pw-template ingress filter mac

configure service template epipe-sap-template egress filter ip
configure service template epipe-sap-template egress filter ipv6
configure service template epipe-sap-template egress filter mac
configure service template epipe-sap-template ingress filter ip
configure service template epipe-sap-template ingress filter ipv6
configure service template epipe-sap-template ingress filter mac

configure service template vpls-sap-template egress filter ip
configure service template vpls-sap-template egress filter ipv6
configure service template vpls-sap-template egress filter mac
configure service template vpls-sap-template ingress filter ip
configure service template vpls-sap-template ingress filter ipv6
configure service template vpls-sap-template ingress filter mac

configure li li-filter-block-reservation li-reserved-block ip-filter
configure li li-filter-block-reservation li-reserved-block ipv6-filter
configure li li-filter-block-reservation li-reserved-block mac-filter
```

**PKI:**

```
configure system security pki ca-profile cmpv2 url
configure system security pki ca-profile ocsp service
```

**QoS:**

```
configure service template epipe-sap-template ingress qos
configure service template epipe-sap-template egress qos

configure service template vpls-sap-template ingress qos
configure service template vpls-sap-template egress qos

configure service pw-template ingress qos
configure service pw-template egress qos
```

**Subscriber Management:**

```
configure service ies subscriber-interface group-interface srrp bfd-enable
configure service vprn subscriber-interface group-interface srrp bfd-enable

configure subscriber-mgmt local-user-db ipoe host host-identification service-id
configure subscriber-mgmt local-user-db ipoe host interface service-id
configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache server
configure subscriber-mgmt local-user-db ipoe host msap-defaults service
configure subscriber-mgmt local-user-db ipoe host retail-service-id

configure subscriber-mgmt local-user-db ppp host interface service-id
configure subscriber-mgmt local-user-db ppp host l2tp group service-id
configure subscriber-mgmt local-user-db ppp host msap-defaults service
configure subscriber-mgmt local-user-db ppp host retail-service-id
```



```
configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-  
snooping mvr from-vpls
```

```
configure service vpls sap msap-defaults service
```

#### Miscellaneous:

```
configure vrrp policy  
configure service vprn interface vrrp bfd-enable
```

```
configure service vprn interface ipv6 vrrp bfd-enable  
configure router l2tp group ppp default-group-interface service-id  
configure router l2tp group tunnel ppp default-group-interface service-id  
configure service vprn l2tp group ppp default-group-interface service-id  
configure service vprn l2tp group tunnel ppp default-group-interface service-id
```

```
configure redundancy multi-chassis peer mc-ring l3-ring in-band-control-  
path service-id  
configure redundancy multi-chassis peer mc-ring l3-ring ring-node connectivity-  
verify service-id  
configure redundancy multi-chassis peer mc-ring ring in-band-control-path service-id  
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-  
verify service-id
```

```
configure open-flow of-switch controller vprn
```

### 3.4.3 Transitioning Between Modes

Depending on the size of the system configuration, transitioning away from classic mode may take several seconds to several minutes while the model-driven database is populated and synchronized to the current configuration. During the transition period, configuration changes are not allowed and service is not affected.

Transitioning to classic mode is immediate with no impact to services on the router.

## 3.5 Configuring the CLI Engine

The CLI engine refers to the CLI environment that is being used in a user session (for example, console, Telnet, or SSH) to configure and operate the router. The CLI engine is either the classic CLI engine or the MD-CLI engine. The following terms are also used:

- preferred CLI engine — the CLI engine that is started at user login
- authorized CLI engine — a CLI engine that a user can switch to (using the CLI engine switch command ("*//*") or where a user can execute commands
- active CLI engine — the CLI engine that is currently in use for a user session

The default preferred CLI engine and authorized CLI engines for a session are determined by the management interface configuration mode, which eliminates the need to explicitly configure the CLI engine. With the use of these dynamic defaults, it is possible to transition between the different configuration modes. [Table 57](#) summarizes the CLI engines for the management interface configuration modes.

**Table 57 Management Interface Configuration Modes and CLI Engines**

Management Interface Configuration Mode	Default Preferred CLI Engine	Default Authorized CLI Engines
classic	classic-cli	classic-cli
model-driven	md-cli	md-cli, classic-cli (read-only)

The preferred CLI engine, and the authorized CLI engines for a session can be changed to use either the classic CLI or the MD-CLI engine.

In the classic CLI, the first engine configured is the preferred CLI engine. The default is **no cli-engine**.

```
A:node-2>config>system>management-interface>cli# cli-engine ?
- cli-engine <engine-type> [<engine-type>...(upto 2 max)]
- no cli-engine

<engine-type>          : classic-cli|md-cli
```

In the MD-CLI, the **cli-engine** parameter is a user-ordered list, and the first engine from that list is configured as the preferred CLI engine. Leaving the **cli-engine** parameter unconfigured (or deleting the **cli-engine** values) maintains or reverts to the dynamic default. [Table 58](#) summarizes the possible actions available with the MD-CLI **cli-engine** configuration.



**Note:** In order for the changes to the **cli-engine** parameter to take effect, log out of the CLI session and start a new session.

**Table 58 MD-CLI cli-engine Configurations**

cli-engine Configuration	Preferred CLI engine	Authorized CLI engines	Description
[classic-cli]	classic-cli	classic-cli	User is restricted to the classic CLI engine
[classic-cli md-cli]	classic-cli	classic-cli, md-cli	User can switch between classic CLI and MD-CLI engines in a session
[md-cli classic-cli]	md-cli	md-cli, classic-cli	User can switch between MD-CLI and classic CLI engines in a session
[md-cli]	md-cli	md-cli	User is restricted to the MD-CLI engine

Refer to the *MD-CLI User Guide* for information about using the MD-CLI to manage to router.



## 3.6 Classic and Model-Driven Management Interfaces Command Reference

### 3.6.1 Command Hierarchies

- [Management Infrastructure Control Commands](#)

#### 3.6.1.1 Management Infrastructure Control Commands

```
config
  — system
    — management-interface
      — cli
        — classic-cli
          — [no] allow-immediate
        — cli-engine {classic-cli | md-cli} [{classic-cli | md-cli}]
        — no cli-engine
        — md-cli
          — [no] auto-config-save
          — environment
            — command-completion
              — [no] enter
              — [no] space
              — [no] tab
            — console
              — length lines
              — width width
            — message-severity-level
              — cli {warning | info}
            — [no] more
            — progress-indicator
              — delay interval
              — [no] shutdown
              — type indicator-type
            — prompt
              — [no] context
              — [no] newline
              — [no] timestamp
              — [no] uncommitted-changes-indicator
            — time-display {local | utc}
          — configuration-mode {classic | mixed | model-driven}
          — schema-path url-string
          — no schema-path
          — yang-modules
            — [no] base-r13-modules
```

- [no] **nokia-modules**
- [no] **nokia-combined-modules**

## 3.6.2 Command Descriptions

### 3.6.2.1 Management Infrastructure Control Commands

#### management-interface

<b>Syntax</b>	<b>management-interface</b>
<b>Context</b>	config>system
<b>Description</b>	This command enables the context to configure management interface parameters.
<b>Parameters</b>	<b>cli</b> — Allows configuration of parameters related to basic CLI commands for datastore infrastructure operation and behavior.

#### cli

<b>Syntax</b>	<b>cli</b>
<b>Context</b>	config>system>management-interface
<b>Description</b>	This command enables the context to configure CLI capabilities.

#### classic-cli

<b>Syntax</b>	<b>classic-cli</b>
<b>Context</b>	config>system>management-interface>cli
<b>Description</b>	This command enables the context to configure parameters related to classic CLI capabilities.

#### allow-immediate

<b>Syntax</b>	[no] <b>allow-immediate</b>
<b>Context</b>	config>system>management-interface>cli>classic-cli

---

<b>Description</b>	<p>This command enables writable access in the <b>configure</b> classic CLI branch.</p> <p>The <b>no</b> form of this command, when configured under the <b>management-interface&gt;cli&gt;classic-cli</b> context, blocks writeable access and configuration changes in the <b>configure</b> classic CLI branch. This causes the running configuration datastore from the <b>configure</b> classic CLI branch to be read-only.</p> <p>This command can be used to enforce the use of candidate configuration and the <b>commit</b> command, instead of allowing immediate mode line-by-line configuration changes.</p>
<b>Default</b>	allow-immediate

## cli-engine

<b>Syntax</b>	<b>cli-engine {classic-cli   md-cli} [{classic-cli   md-cli}]</b> <b>no cli-engine</b>
<b>Context</b>	config>system>management-interface>cli
<b>Description</b>	<p>This command configures the system-wide CLI engine. You can configure one or both engines.</p> <p>In order for the changes to the <b>cli-engine</b> parameter to take effect, log out of the CLI session and start a new session.</p>
<b>Parameters</b>	<p><b>classic-cli</b> — Specifies the classic CLI.</p> <p><b>md-cli</b> — Specifies the MD-CLI.</p>

## md-cli

<b>Syntax</b>	<b>md-cli</b>
<b>Context</b>	config>system>management-interface>cli
<b>Description</b>	This command enters the context to configure MD-CLI capabilities.

## auto-config-save

<b>Syntax</b>	<b>[no] auto-config-save</b>
<b>Context</b>	config>system>management-interface>cli>md-cli
<b>Description</b>	This command enables or disables the functionality to automatically save the configuration as part of a commit operation.

---

## environment

<b>Syntax</b>	<b>environment</b>
<b>Context</b>	config>system>management-interface>cli>md-cli
<b>Description</b>	This command enters the context to configure MD-CLI session environment parameters.

## command-completion

<b>Syntax</b>	<b>command-completion</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment
<b>Description</b>	This command configures keystrokes to trigger command completion.

## enter

<b>Syntax</b>	<b>[no] enter</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment>command-completion
<b>Description</b>	This command enables completion on the enter character.  The <b>no</b> form of this command reverts to the default value.
<b>Default</b>	enter

## space

<b>Syntax</b>	<b>[no] space</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment>command-completion
<b>Description</b>	This command enables completion on the space character.  The <b>no</b> form of this command reverts to the default value.
<b>Default</b>	space

## tab

<b>Syntax</b>	<b>[no] tab</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment>command-completion



**Description** This command enables completion on the tab character.  
The **no** form of this command reverts to the default value.

**Default** tab

## console

**Syntax** console

**Context** config>system>management-interface>cli>md-cli>environment

**Description** This command enables the context to configure console parameters.

## length

**Syntax** length *lines*

**Context** config>system>management-interface>cli>md-cli>environment>console

**Description** This command configures the set number of lines displayed on screen.

**Default** length 24

**Parameters** *lines* — Specifies the number of lines displayed in the console window.

**Values** 24 to 512

## width

**Syntax** width *width*

**Context** config>system>management-interface>cli>md-cli>environment>console

**Description** This command configures the set number of columns displayed on screen.

**Default** width 80

**Parameters** *width* — Specifies the number of columns displayed in the console window.

**Values** 80 to 512

## message-severity-level

**Syntax** message-severity-level

**Context** config>system>management-interface>cli>md-cli>environment

---

<b>Description</b>	This command configures the message severity level.
--------------------	---

## cli

<b>Syntax</b>	<b>cli</b> { <b>warning</b>   <b>info</b> }
<b>Context</b>	config>system>management-interface>cli>md-cli>environment>message-severity-level
<b>Description</b>	This command specifies the threshold for CLI messages.
<b>Default</b>	cli info
<b>Parameters</b>	<b>warning</b> — Specifies that WARNING messages are displayed but INFO messages are suppressed. <b>info</b> — Specifies that INFO messages and WARNING messages are displayed.

## more

<b>Syntax</b>	[ <b>no</b> ] <b>more</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment
<b>Description</b>	This command configures pagination of the output text.  The <b>no</b> form of this command reverts to the default value.
<b>Default</b>	more

## progress-indicator

<b>Syntax</b>	<b>progress-indicator</b>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment
<b>Description</b>	This command enables the context to configure progress indicator parameters.

## delay

<b>Syntax</b>	<b>delay</b> <i>interval</i>
<b>Context</b>	config>system>management-interface>cli>md-cli>environment>progress-indicator
<b>Description</b>	This command sets the delay before the progress indicator is displayed in the MD-CLI.
<b>Default</b>	delay 500

---

**Parameters**    *interval* — Specifies the delay interval, in milliseconds.  
**Values**        1 to 10000

## shutdown

**Syntax**        **[no] shutdown**

**Context**        config>system>management-interface>cli>md-cli>environment>progress-indicator

**Description**    This command controls whether the progress indicator is active during command execution.  
                     The **no** form of this command reverts to the default value.

**Default**        no shutdown

## type

**Syntax**        **type** *indicator-type*

**Context**        config>system>management-interface>cli>md-cli>environment>progress-indicator

**Description**    This command specifies the type of progress indicator used in the MD-CLI.

**Default**        type dots

**Parameters**    *indicator-type* — Specifies the progress indicator type.  
**Values**        **dots:** displays the progress indicator as dynamically changing dots

## prompt

**Syntax**        **prompt**

**Context**        config>system>management-interface>cli>md-cli>environment

**Description**    This command enables the context to configure prompt parameters.

## context

**Syntax**        **[no] context**

**Context**        config>system>management-interface>cli>md-cli>environment>prompt

**Description**    This command displays the current command context in the prompt.  
                     The **no** form of this command suppresses the current command context in the prompt.

---

**Default** context

## newline

**Syntax** [no] newline

**Context** config>system>management-interface>cli>md-cli>environment>prompt

**Description** This command displays a new line before the first prompt line.  
The **no** form of this command suppresses the new line before the first prompt line.

**Default** newline

## timestamp

**Syntax** [no] timestamp

**Context** config>system>management-interface>cli>md-cli>environment>prompt

**Description** This command displays the timestamp before the first prompt line.  
The **no** form of this command suppresses the timestamp before the first prompt line.

**Default** timestamp

## uncommitted-changes-indicator

**Syntax** [no] uncommitted-changes-indicator

**Context** config>system>management-interface>cli>md-cli>environment>prompt

**Description** This command displays the change indicator.  
The **no** form of this command suppresses the change indicator.

**Default** uncommitted-changes-indicator

## time-display

**Syntax** time-display {local | utc}

**Context** config>system>management-interface>cli>md-cli>environment

**Description** This command configures whether the time is displayed in coordinated Universal Time (UTC) or local time (as configured in **config>system>time**).

---

<b>Default</b>	time-display local
<b>Parameters</b>	<b>local</b> — Specifies that the local time zone is used. <b>utc</b> — Specifies that UTC is used.

## configuration-mode

<b>Syntax</b>	<b>configuration-mode {classic   mixed   model-driven}</b>
<b>Context</b>	config>system>management-interface
<b>Description</b>	This command controls which management interfaces are used for editing and changing the configuration of the router.
<b>Default</b>	configuration-mode classic
<b>Parameters</b>	<b>classic</b> — Enables editing of router configuration via classic CLI and SNMP management interfaces, but not using model-driven interfaces. <b>model-driven</b> — Enables editing of router configuration via model-driven management interfaces (NETCONF with 'Nokia' YANG models, MD-CLI or gRPC), but not using classic interfaces. <b>mixed</b> — Enables editing of router configuration using a mix of classic and/or model-driven management interfaces (with some restrictions and limitations).

## schema-path

<b>Syntax</b>	<b>schema-path <i>url-string</i></b> <b>no schema-path</b>
<b>Context</b>	config>system>management-interface
<b>Description</b>	This command enables the definition a schema-path where the SR OS YANG modules are manually copied by the user prior to using a <get-schema> request
<b>Default</b>	"cf3:/YANG"
<b>Parameters</b>	<i>url-string</i> — Specifies the schema path URL up to 180 characters.

## base-r13-modules

<b>Syntax</b>	<b>[no] base-r13-modules</b>
<b>Context</b>	config>system>management-interface>yang-modules

---

<b>Description</b>	This command enables or disables support of the Base-R13 YANG modules in the SR OS NETCONF server. If the Base-R13 modules are disabled, then the NETCONF requests, which reference the Base-R13 modules, return an error, and when a NETCONF client establishes a new session, the Base-R13 modules are not advertised in the SR OS <i>hello</i> . When <b>management-interface configuration-mode</b> is set to <b>model-driven</b> , attempts to modify the configuration using the Base-13 configuration modules or namespace via NETCONF results in errors, even if <b>base-r13-modules</b> is enabled.
<b>Default</b>	base-r13-modules

## nokia-modules

<b>Syntax</b>	[no] <b>nokia-modules</b>
<b>Context</b>	config>system>management-interface>yang-modules
<b>Description</b>	This command enables or disables support of the Nokia YANG modules in the SR OS NETCONF server. If the Nokia modules are disabled, then the NETCONF requests, which reference the Nokia modules, return an error, and when a NETCONF client establishes a new session, the Nokia modules are not advertised in the SR OS <i>hello</i> . When <b>management-interface configuration-mode</b> is set to <b>classic</b> , attempts to access (read or write) the configuration using the Nokia configuration modules or namespace via NETCONF results in errors, even if <b>nokia-modules</b> is enabled.
<b>Default</b>	nokia-modules

## nokia-combined-modules

<b>Syntax</b>	[no] <b>nokia-combined-modules</b>
<b>Context</b>	config>system>management-interface>yang-modules
<b>Description</b>	<p>This command enables support of the combined NOKIA YANG files for both configuration and state data.</p> <p>This command is mutually exclusive with the <b>nokia-modules</b> command. They cannot be both enabled at the same time where the validation is done at commit time. The default configuration is <b>nokia-modules</b> and <b>no nokia-combined-modules</b>.</p> <p>The <b>no</b> form of this command disables support of the combined NOKIA YANG files for both configuration and state data.</p>
<b>Default</b>	no nokia-combined-modules

## 3.7 Classic and Model-Driven Management Interfaces Show Command Reference

### 3.7.1 Command Hierarchies

- [Management Infrastructure Show Commands](#)

#### 3.7.1.1 Management Infrastructure Show Commands

```
show
  — system
    — management-interface
      — configuration-sessions
      — datastore-locks [detail]
```

### 3.7.2 Command Descriptions

#### 3.7.2.1 Management Infrastructure Show Commands

##### management-interface

<b>Syntax</b>	management-interface
<b>Context</b>	show>system
<b>Description</b>	This command enters the context to display management interface information.

##### configuration-sessions

<b>Syntax</b>	configuration-sessions
<b>Context</b>	show>system>management-interface
<b>Description</b>	This command displays configuration sessions information.

**Output** The following output displays configuration session information. [Table 59](#) describes the output fields.

### Sample Output

```
(pr) []
A:admin@node-1# show system management-interface configuration-sessions
=====
Session ID  Region                Datastore                Lock State
Username
Session Type                Session Mode                Idle Time
From
-----
#65         configure            Candidate                Unlocked
admin       Private                0d 00:00:00
MD-CLI     192.168.255.255
66         configure            Candidate                Unlocked
admin       Private                0d 00:05:41
MD-CLI     192.168.255.255
67         configure            Candidate                Unlocked
admin       Private                0d 00:05:08
MD-CLI     192.168.255.255
68         configure            Candidate                Unlocked
admin       Read-Only              0d 00:02:25
MD-CLI     192.168.255.255
69         configure            Candidate, Running       Locked
admin       Exclusive               0d 00:01:54
MD-CLI     192.168.255.255
-----
Number of sessions: 5
'#' indicates the current active session
=====
```

**Table 59** Configuration-sessions Output Fields

Label	Description
Session ID	The session ID.
Region	The region or scope that the datastore belongs to.
Datastore	Datastores that can be locked. For example: Running and Candidate.
Lock State	Locked — Indicates the session is in a locked state. Unlocked — Indicates the session is in an unlocked state.
Username	The name of the user.
Session Mode	Exclusive — An exclusive session. Global — A shared session. Private — A private session. Private Exclusive — A private exclusive session. Read-Only — A read-only session.



**Table 59 Configuration-sessions Output Fields (Continued)**

Label	Description (Continued)
Idle Time	The idle time of the session.
Session Type	NETCONF — Indicates a NETCONF session is running. MD-CLI — Indicates an MD-CLI session is running. gRPC — Indicates a gRPC session is running. SNMP — Indicates an SNMP session is running. Classic CLI — Indicates a classic CLI session is running. System — Indicates a system (EHS or CRON) session is running.
From	The originating IP address.

## datastore-locks

<b>Syntax</b>	<b>datastore-locks [detail]</b>
<b>Context</b>	show>system>management-interface
<b>Description</b>	This command displays datastore locks information.
<b>Parameters</b>	<b>detail</b> — Displays session-specific information.
<b>Output</b>	The following output displays detail datastore locks information for all datastores. <a href="#">Table 60</a> describes the output fields.

### Sample Output

```
[ ]
A:admin@node-1# show system management-interface datastore-locks detail
=====
Session ID  Region      Datastore      Lock State
Username    Session Mode  Idle Time
Session Type From
-----
23          configure   Running        Locked
admin       Exclusive    0d 00:00:11
NETCONF    192.168.255.255
26          configure   Running        Unlocked
test1       Global       0d 00:00:11
MD-CLI     192.168.255.255
-----
Number of sessions: 2
'#' indicates the current active session
=====
```

**Table 60**      **Datastore-locks Output Fields**

Label	Description
Session ID	The session ID.
Region	The region or scope that the datastore belongs to.
Datastore	Datastores that can be locked. For example: Running and Candidate.
Lock State	Locked — Indicates the session is in a locked state. Unlocked — Indicates the session is in an unlocked state.
Username	The name of the user.
Session Mode	Global — A shared session. Exclusive — An exclusive session.
Idle Time	The idle time of the session.
Session Type	NETCONF — Indicates a NETCONF session is running. MD-CLI — Indicates an MD-CLI session is running. gRPC — Indicates a gRPC session is running. SNMP — Indicates an SNMP session is running. Classic CLI — Indicates a classic CLI session is running. System — Indicates a system (EHS or CRON) session is running.
From	The originating IP address.

---

## 4 SNMP

### 4.1 SNMP Overview

This section provides an overview of the Simple Network Management Protocol (SNMP).

#### 4.1.1 SNMP Architecture

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

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

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

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

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

---

## 4.1.2 Management Information Base

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

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

## 4.1.3 SNMP Protocol Operations

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

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

## 4.1.4 SNMP Versions

The agent supports multiple versions of the SNMP protocol.

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

---

## 4.1.5 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 sub-set of the agent's managed objects can be accessed by the requester. It also defines what type of access is allowed: read-only or read-write.

The use of community strings provide minimal security and context checking for both agents and managers that receive requests and initiate trap operations. A community string is a text string that acts like a password to permit access to the agent on the router.

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

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

## 4.1.6 User-Based Security Model Community Strings

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

---

## 4.1.7 Views

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

OIDs are organized in a hierarchical tree with specific values assigned to different organizations. A view defines a subset of the agent'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, and so on). 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 Nokia SNMP agent associates SNMPv1 and SNMPv2c community strings with a SNMPv3 view.

## 4.1.8 Access Groups

Access groups associate a user group and a security model to the views the group can access. An access group is defined by a unique combination of a group name, security model (SNMPv1, SNMPv2c, or SNMPv3), and security level (no-authorization-no privacy, authorization-no-privacy, or privacy).

An access group, in essence, is a template which defines a combination of access privileges and views. A group can be associated to one or more network users to control their access privileges and views.

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.

### 4.1.9 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](#)).

### 4.1.10 Per-VPRN Logs and SNMP Access

Configuration of VPRN-specific logs (with VPRN-specific syslog destinations, SNMP trap, notification groups, and so on) 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 VPRN 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 VPRN. For example, walking the ifTable (IF-MIB) using the community configured for VPRN 5 will return counters and status for VPRN 5.

---

### 4.1.11 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”).



---

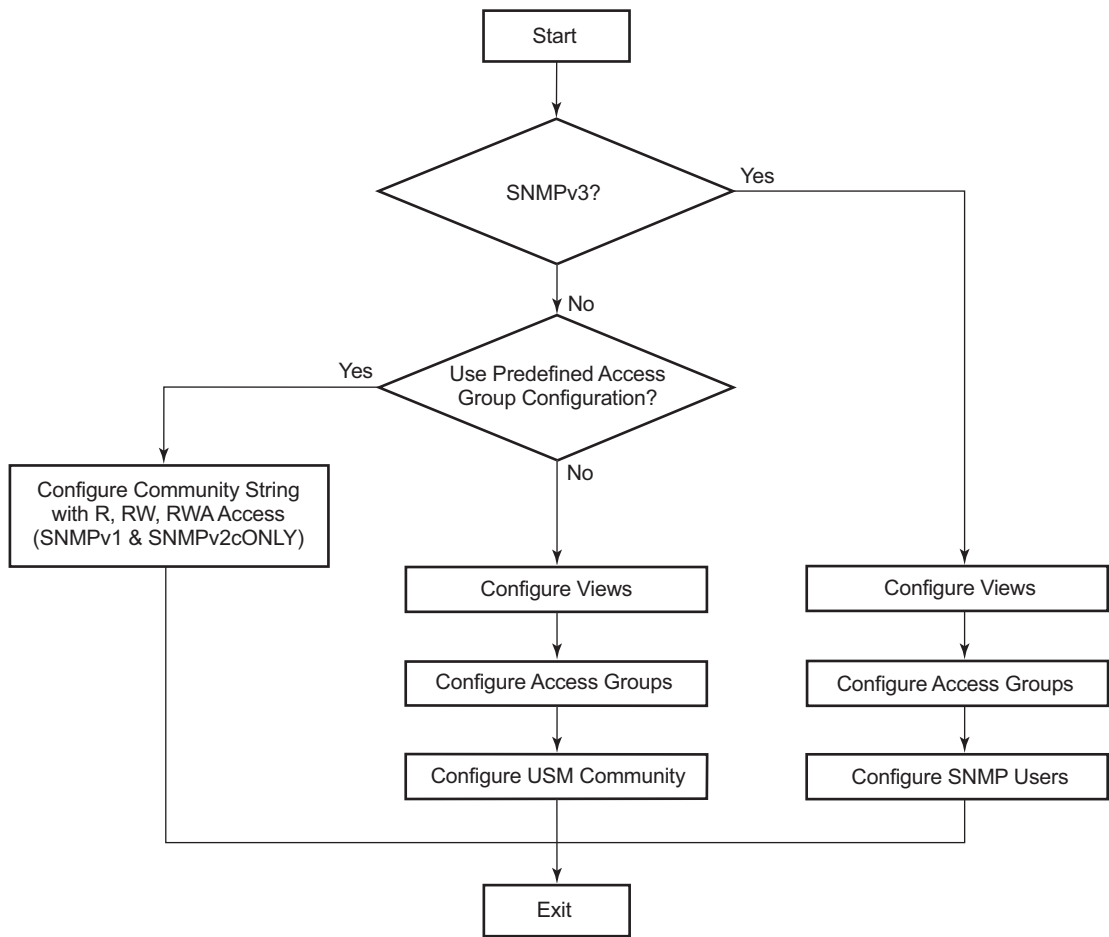
## 4.2 SNMP Versions

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

**Figure 14**     **SNMPv1 and SNMPv2c Configuration and Implementation Flow**



al\_0203

---

## 4.3 Configuration Notes

This section describes SNMP configuration restrictions.

### 4.3.1 General

- To avoid management systems attempting to manage a partially booted system, SNMP will remain in a shut down state if the configuration file fails to complete during system startup. While shutdown, SNMP gets and sets are not processed. However, notifications are issued if an SNMP trap group has been configured. 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.



---

## 4.4 Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

### 4.4.1 SNMP Configuration Overview

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

#### 4.4.1.1 Configuring SNMPv1 and SNMPv2c

Nokia routers are based on SNMPv3. To use the routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three 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.

#### 4.4.1.2 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

## 4.4.2 Basic SNMP Security Configuration

This section provides information to configure SNMP parameters and provides examples of common configuration tasks. The minimal SNMP parameters are:

For SNMPv1 and SNMPv2c:

- Configure community string parameters.

For SNMPv3:

- Configure view parameters
- Configure SNMP group
- Configure access parameters
- Configure user with SNMP parameters

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

```

## 4.4.3 Configuring SNMP Components

### 4.4.3.1 Configuring a Community String

SNMPv1 and SNMPv2c community strings are used to define the relationship between an SNMP manager and agent. The community string acts like a password to permit access to the agent. The access granted with a community string is restricted to the scope of the configured group.

One or more of these characteristics associated with the string can be specified:

- Read-only, read-write, and read-write-all permission for the MIB objects accessible to the community.
- The SNMP version, SNMPv1 or SNMPv2c.

Default access features are pre-configured by the agent for SNMPv1/SNMPv2c.

Use the following CLI syntax to configure community options:

```

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#

```

### 4.4.3.2 Configuring View Options

Use the following CLI syntax to configure view options:

**CLI Syntax:**   config>system>security>snmp  
                  view view-name subtree oid-value  
                  mask mask-value [type {included | excluded}]

The following 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 "L1a.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both
-----
*A:cses-A13>config>system>security>snmp#
```

### 4.4.3.3 Configuring Access Options

The **access** command creates an association between a user group, a security model and the views that the user group can access. Access must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Use the following 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-Al3>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#

```

#### 4.4.3.4 Configuring USM Community Options

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

By default, the OS implementation of SNMP uses SNMPv3. However, to implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

**CLI Syntax:**

```

config>system>security>snmp
usm-community community-string group group-name

```

The following displays a SNMP community configuration example:

```

A:ALA-1>config>system>security>snmp# info
-----
view "testview" subtree "1"
    mask ff
    exit
    view "testview" subtree "1.3.6.1.2"
        mask ff type excluded
    exit
    access group "test" security-model usm security-level auth-no-pr
ivacy read "testview" write "testview" notify "testview"
    community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
    community "Lla.RtAyRW2" hash2 r version v2c
    community "r0a159kIOfg" hash2 r version both
-----
A:ALA-1>config>system>security>snmp#

```

The group **grouptest** was configured in the **config>system>security>snmp>access** CLI context.

#### 4.4.3.5 Configuring Other SNMP Parameters

Use the following CLI syntax to modify the system SNMP options:

**CLI Syntax:**

```

config>system>snmp
engineID engine-id
general-port port
packet-size bytes
no shutdown

```

The following example displays the system SNMP default values:

```

A:ALA-104>config>system>snmp# info detail
-----
shutdown
engineID "0000xxxx000000000xxxxx00"
packet-size 1500
general-port 161
-----
A:ALA-104>config>system>snmp#

```

## 4.5 SNMP Configuration Command Reference

### 4.5.1 Command Hierarchies

- [SNMP System Commands](#)
- [SNMP Security Commands](#)

#### 4.5.1.1 SNMP System Commands

```

config
  — system
    — snmp
      — engineID engine-id
      — no engineID
      — general-port port
      — no general-port
      — packet-size bytes
      — no packet-size
      — streaming
        — [no] shutdown
      — [no] shutdown
  
```

#### 4.5.1.2 SNMP Security Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* 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**]
- **[no] src-access-list** *list-name*
  - **src-host** *host-name* **address** *ip-address*
  - **no src-host** *host-name*
- **usm-community** *community-string* **group** [**hash**|**hash2**] *group-name* [*src-access-list list-name*]
- **no usm-community** *community-string* [**hash**|**hash2**]
- **view** *view-name* **subtree** *oid-value*
- **no view** *view-name* [**subtree** *oid-value*]
  - **mask** *mask-value* [**type** {**included** | **excluded**}]
  - **no mask**

The following commands configure user-specific SNMP features. Refer to the **Security** section for CLI syntax and command descriptions.

```

config
  — system
    — security
      — [no] user user-name
      — [no] snmp
        — authentication {[none] | [[hash] {md5 key-1 | sha key-1}
          privacy {none | des-key | aes-128-cfb-key key-2}]
        — authentication group-name
        — [no] group group-name

```

## 4.5.2 Command Descriptions


- [SNMP System Commands](#)
- [SNMP Security Commands](#)

### 4.5.2.1 SNMP System Commands

snmp

<b>Syntax</b>	<b>snmp</b>
<b>Context</b>	config>system config>system>security
<b>Description</b>	This command creates the context to configure SNMP parameters.

## 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> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <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> </div> </div> <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> — Specifies 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> <b>no general-port</b>
<b>Context</b>	config>system>snmp
<b>Description</b>	<p>This command configures the port number used by this node to receive SNMP request messages and to send replies. SNMP notifications generated by the agent are sent from the port specified in the <b>config&gt;log&gt;snmp-trap-group&gt;trap-target</b> CLI command.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>

---

<b>Default</b>	general-port 161
<b>Parameters</b>	<i>port-number</i> — Specifies port number used to send SNMP traffic other than traps.
<b>Values</b>	1 to 65535

## packet-size

<b>Syntax</b>	<b>packet-size</b> <i>bytes</i> <b>no packet-size</b>
<b>Context</b>	config>system>snmp
<b>Description</b>	This command configures the maximum SNMP packet size generated by this node.  The <b>no</b> form of this command restores the default value.
<b>Default</b>	packet-size 1500
<b>Parameters</b>	<i>bytes</i> — Specifies the SNMP packet size in bytes.
<b>Values</b>	484 to 9216

## streaming

<b>Syntax</b>	<b>streaming</b>
<b>Context</b>	config>system>snmp
<b>Description</b>	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>	This command administratively disables proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes.  The <b>no</b> form of the command administratively re-enables SNMP request/response bundling and TCP-based transport mechanism.
<b>Default</b>	shutdown

## 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>	no shutdown

### 4.5.2.2 SNMP Security Commands

## 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.

## 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>	This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Access groups are used by the `usm-community` command.

Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the [community](#)).

Default access group configurations cannot be modified or deleted.

To remove the user group with associated, security model(s), and security level(s), use:

**no access group** *group-name*

To remove a security model and security level combination from a group, use:

**no access group** *group-name* **security-model** {**snmpv1** | **snmpv2c** | **usm**} **security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}

#### Parameters

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

**security-model** {**snmpv1** | **snmpv2c** | **usm**} — Specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.

**security-level** {**no-auth-no-priv** | **auth-no-priv** | **privacy**} — Specifies the required authentication and privacy levels to access the views configured in this node.

**security-level no-auth-no-privacy** — Specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the **none** option.

**security-level auth-no-privacy** — Specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the **group** and the **user** must be configured for authentication.

**security-level privacy** — Specifies that both authentication and privacy (encryption) is required. When this option is configured, both the **group** and the user must be configured for **authentication**. The user must also be configured for **privacy**.

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

The *context-name* is treated as either a full context-name string or a context name prefix depending on the keyword specified (**exact** or **prefix**).

**prefix-match** — Specifies the context name **prefix-match** keywords, **exact** or **prefix**. This parameter applies only to the 7750 SR.

The VPRN context names begin with a **vprn** prefix. The numerical value is associated with the service ID that the VPRN was created with and identifies the service in the service domain. For example, when a new VPRN service is created such as **config>service>vprn 2345 customer 1**, a VPRN with context name **vprn2345** is created.

The **exact** keyword specifies that an exact match between the context name and the prefix value is required. For example, when context **vprn2345 exact** is entered, matches for only **vprn2345** are considered.



The **prefix** keyword specifies that only a match between the prefix and the starting portion of context name is required. If only the **prefix** keyword is specified, simple wildcard processing is used. For example, when context vprn prefix is entered, all **vprn** contexts are matched.

**Default**      **exact**

*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**

*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

*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> ] <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 restores the default values, in which 20 failed SNMP attempts are allowed in a 5 minute period with a 10 minute lockout for the host if exceeded.</p>
<b>Default</b>	attempts 20 time 5 lockout 10
<b>Parameters</b>	<p><i>count</i> — Specifies the number unsuccessful SNMP attempts allowed for the specified <b>time</b>.</p> <p><b>Values</b>      1 to 64</p> <p><i>minutes1</i> — Specifies period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out.</p> <p><b>Values</b>      0 to 60</p>

*minutes2* — Specifies the lockout period in minutes where the host is not allowed to login. When the host exceeds the attempted count times in the specified time, then that host is locked out from any further login attempts for the configured time period.

**Values** 0 to 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> ] [ <b>src-access-list</b> <i>list-name</i> ] <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 <a href="#">usm-community</a> command.</p> <p>When configured, community implies a security model for SNMPv1 and SNMPv2c only.</p> <p>For SNMPv3 security, the <a href="#">access group</a> command must be configured.</p> <p>The <b>no</b> form of the command removes the specified community string.</p>
<b>Parameters</b>	<p><i>community-string</i> — Configures the SNMPv1 and/or SNMPv2c community string.</p> <p><b>Values</b></p> <ul style="list-style-type: none"> <li>community-string — 32 characters maximum</li> <li>hash-key — 33 characters maximum</li> <li>hash2-key — 96 characters maximum</li> </ul> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the <b>hash2</b> encrypted variable cannot be copied and pasted. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified.</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, using the internal "snmp-ro" access group and the "no-security" snmp view.</li> <li><b>rw</b> — Grants read and write access to all objects in the MIB, using the internal "snmp-rw" access group and the "no-security" snmp view.</li> <li><b>rwa</b> — Grants read and write access to all objects in the MIB, including security, using the internal snmp-rwa access group and the iso snmp view.</li> </ul>

**mgmt** — Assigns a unique SNMP community string for SNMP access via the management router instance. This community uses the internal snmp-mgmt access group and the mgmt snmp view.

**vppls-mgmt** — Assigns a unique SNMP community string for SNMP access via the vppls-management router instance. This community uses the internal snmp-vppls-mgmt access group and mgmt-view snmp view.

**version {v1 | v2c | both}** — Configures the scope of the community string to be for SNMPv1, SNMPv2c, or both SNMPv1 and SNMPv2c access.

**Default** both

**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, usm-community, or VPRN SNMP community instances can reference the same src-access-list.

## src-access-list

<b>Syntax</b>	<b>src-access-list</b> <i>list-name</i> <b>no src-access-list</b> <i>list-name</i>
<b>Context</b>	config>system>security>snmp
<b>Description</b>	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.

An src-address-list referenced by one or more [community](#) instances is used to verify the source IP addresses of an SNMP request using the **community** 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 **community**, then the source IP address in the packet would be validated against the src-address-list configured for the **community**. 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 message’s source IP address does not match the *ip-address* of any of the **src-hosts** contained in the list, then the request will be discarded and logged as an SNMP authentication failure.

Using src-access-list 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 NSP NFM-P, at the top of the list.

A maximum of 16 source access lists can be configured. Each source access lists can contain a maximum of 16 source hosts.

The **no** form of this command removes the named src-access-list. You cannot remove an **src-access-list** that is referenced by one or more **community** instances.

---

**Parameters** *list-name* — Configures the name or key of the **src-access-list**. The *list-name* parameter must begin with a letter (a-z or A-Z).

## src-host

**Syntax** **src-host** *host-name* **address** *ip-address*  
**no src-host** *host-name*

**Context** config>system>security>snmp>src-access-list

**Description** This command is used to configure a source IP address entry that can be used to validate SNMPv1 and SNMPv2c requests.

The **no** form of this command removes the specified entry.

**Parameters** *host-name* — Configures the name of the **src-host** entry.  
*ip-address* — Configures an allowed source address for SNMP requests. This can be an IPv4 or IPv6 address.

**Values**      ipv4-address: a.b.c.d  
                  ipv6-address: x:x:x:x:x:x:x  
                  x:x:x:x:x:d.d.d.d  
                  x: [0..FFFF]H  
                  d: [0..255]D

## usm-community

**Syntax** **usm-community** *community-string* [**hash**|**hash2**] **group** *group-name* [*src-access-list list-name*]  
**no usm-community** *community-string* [**hash**|**hash2**]

**Context** config>system>security>snmp

**Description** This command is used to associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

Nokia's SR OS implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (Version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views which specify more specific OIDs (MIB objects in the subtree) can be configured.

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

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

*group* — Specifies the group that governs the access rights of this community string. This group must be configured first in the **config>system>security>snmp>access group** context.

*list-name* — Specifies the usm-community to reference a specific src-access-list that will be used to validate the source IP address of all received SNMP requests that use this usm-community. Multiple **community**, **usm-community**, or **vpn snmp community** instances can reference the same **src-access-list**.


## view

<b>Syntax</b>	<b>view</b> <i>view-name</i> <b>subtree</b> <i>oid-value</i> <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 <a href="#">mask</a> 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> — Specifies a character view name up to 32 characters in length.</p> <p><i>oid-value</i> — Specifies 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>

## mask

**Syntax**    **mask** *mask-value* [**type** {**included** | **excluded**}]

**no mask**

<b>Context</b>	config>system>security>snmp>view view-name				
<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 vacmViewTreeFamilyType in the entry whose value of vacmViewTreeFamilySubtree has the most sub-identifiers.</p> <p>The <b>no</b> form of this command removes the mask from the configuration.</p>				
<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 1s)</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> <div><p><b>Note:</b> 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></div> <p><b>type</b> — Specifies to include or exclude MIB subtree objects.</p> <table><tr><td><b>Values</b></td><td><p><b>included</b> - All MIB subtree objects that are identified with a 1 in the mask are available in the view.</p><p><b>excluded</b> - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view.</p></td></tr><tr><td><b>Default</b></td><td><b>included</b></td></tr></table>	<b>Values</b>	<p><b>included</b> - All MIB subtree objects that are identified with a 1 in the mask are available in the view.</p> <p><b>excluded</b> - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view.</p>	<b>Default</b>	<b>included</b>
<b>Values</b>	<p><b>included</b> - All MIB subtree objects that are identified with a 1 in the mask are available in the view.</p> <p><b>excluded</b> - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view.</p>				
<b>Default</b>	<b>included</b>				

## 4.6 SNMP Show Command Reference

### 4.6.1 Command Hierarchies

#### 4.6.1.1 Show Commands

```
show
  — snmp
    — counters
    — streaming
      — counters
  — system
    — information
    — security
      — access-group [group-name]
      — authentication [statistics]
      — 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]
```

### 4.6.2 Command Descriptions

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### 4.6.2.1 Show Commands

##### counters

**Syntax**     **counters**

**Context**    show>snmp

**Description** This command displays SNMP counters information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.

**Output** The following example displays SNMP counter information.

Table 61 describes the SNMP counters output fields.

Sample Output

```
A:ALA-1# show snmp counters
=====
SNMP counters:
=====
  in packets : 463
-----
    in gets      : 93
    in getnexts  : 0
    in sets      : 370

  out packets : 463
-----
    out get responses : 463
    out traps         : 0

  variables requested : 33
  variables set       : 497
=====
A:ALA-1#
```

Table 61 Show 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.



**Table 61 Show Counters Output Fields (Continued)**

Label	Description
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.

## streaming

<b>Syntax</b>	<b>streaming</b>
<b>Context</b>	show>snmp
<b>Description</b>	This command enables the context to display streaming counters information.

## counters

<b>Syntax</b>	<b>counters</b>
<b>Context</b>	show>snmp>streaming
<b>Description</b>	This command displays counters information for the proprietary SNMP streaming protocol.
<b>Output</b>	The following is an example of SNMP streaming counters information.

[Table 62](#) describes the SNMP streaming counters output fields.

### Sample Output

```
*A:Dut-B# show snmp streaming counters
=====
STREAMING counters:
=====
      in getTables   : 772
      in getManys    : 26
-----
      out responses  : 848
=====
```

**Table 62 Show Streaming 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.

**Table 62 Show Streaming Counters Output Fields (Continued)**

Label	Description
out responses	Displays the number of response packets sent.

## 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>	The following displays an example of system information.

[Table 63](#) describes system information output fields.

### Sample Output

The following is an output example of the 7950 XRS:

```
*A:7950 XRS-20# show system information
=====
System Information
=====
System Name           : 7950 XRS-20
System Type           : 7950 XRS-20
Chassis Topology      : Standalone
System Version        : C-10.0.B1-103
System Contact        :
System Location       :
System Coordinates    :
System Active Slot    : A
System Up Time        : 19 days, 18:43:59.66 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f0000ac9fff000000
SNMP Engine Boots     : 1
SNMP Max Message Size : 1500
SNMP Admin State      : Disabled
SNMP Oper State       : Disabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State       : N/A

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

BOF Source            : cf3:
Image Source          : primary
Config Source         : primary
Last Booted Config File: ftp://*:kandhcp214/tftpboot/bksimgrp31/images/bksim3
                        106/bksim3106.cfg
Last Boot Cfg Version  : WED MAY 23 11:58:26 2012 UTC
Last Boot Config Header: # TiMOS-C-14.0.B1-217 cpm/
```

```
x86_64 Nokia 7950 XRS Copyright (c)
    2000-2016 Nokia. # All rights
    reserved. All use subject to applicable license
    agreements. # Built on Wed Jul 13 19:09:32 PDT 2016
    by builder in /rel14.0/b1/B1-217/panos/main

Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-C-0.0.I3339 cpm/i386 Nokia 7950 XRS
    Copyright (c) 2000-2016 Nokia. # All rights
    reserved. All use subject to applicable license
    agreements. # Built on Tue May 22 18:46:56 PDT 2016
    by builder in /rel14.0/I3339/panos/main # Generated
    WED MAY 23 11:58:26 2016 UTC

Last Saved Config      : ftp://*:kandhcp214/tftpboot/bksimgrp31/images/bksim3
    106/bksim3106.cfg

Time Last Saved        : 2012/05/28 10:38:31
Changes Since Last Save: Yes
User Last Modified     : admin
Time Last Modified     : 2012/06/06 17:06:15
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script          : N/A
Cfg-OK Script Status   : not used
Cfg-Fail Script        : N/A
Cfg-Fail Script Status : not used

Management IP Addr     : 10.120.214.159/24
Primary DNS Server     : 10.120.252.56
Secondary DNS Server   : 10.120.252.48
Tertiary DNS Server    : 10.120.252.49
DNS Domain             : labs.ca.nokia.com
DNS Resolve Preference : ipv4-only
BOF Static Routes      :
    To                Next Hop
    10.244.0.0/16      10.120.214.1
    10.120.0.0/16      10.120.214.1

ICMP Vendor Enhancement: Disabled
=====
```

**Table 63**      **Show System Information Output Fields**

Label	Description
System Name	Displays the name configured for the device.
System Type	Indicates the SR OS platform type (for example, 7750 SR-12).

**Table 63 Show System Information Output Fields (Continued)**

Label	Description
Chassis Topology	<p>Indicates the inter-chassis topology mode in which the system is operating.</p> <p><b>Standalone</b> indicates that the system is comprised of a single physical router chassis.</p> <p><b>Extended</b> (XRS-40) on a 7950 XRS-based system indicates that two router chassis are connected together in a back-to-back topology with no additional switch fabric chassis. An extended chassis topology is comprised of two XRS-20 chassis and is also known as an XRS-40 system.</p>
System Contact	Displays the text string that identifies the contact name for the device.
System Location	Displays the text string that identifies the location of the device.
System Coordinates	Displays the text string that identifies the system coordinates for the device location. For example, "37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.
System Up Time	Displays the time since the last reboot.
SNMP Port	Displays the port which SNMP sends responses to management requests.
SNMP Engine ID	Displays the ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node.
SNMP Max Message Size	Displays the maximum size SNMP packet generated by this node.
SNMP Admin State	Enabled — Indicates that SNMP is administratively enabled.
	Disabled — Indicates that administratively disabled.
SNMP Oper State	Enabled — Indicates that operationally enabled.
	Disabled — Indicates that operationally disabled.
SNMP Index Boot Status	Persistent — Indicates that persistent indexes at the last system reboot was enabled.
	Disabled — Indicates that persistent indexes at the last system reboot was disabled.

**Table 63 Show System Information Output Fields (Continued)**

Label	Description
SNMP Sync State	Displays the state when the synchronization of configuration files between the primary and secondary CPMs finish.
Telnet/SSH/FTP Admin	Displays the administrative state of the Telnet, SSH, and FTP sessions.
Telnet/SSH/FTP Oper	Displays the operational state of the Telnet, SSH, and FTP sessions.
BOF Source	Displays the boot location of the BOF.
Image Source	primary — Specifies whether the image was loaded from the primary location specified in the BOF. secondary — Specifies whether the image was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the image was loaded from the tertiary location specified in the BOF.
Config Source	primary — Specifies whether the configuration was loaded from the primary location specified in the BOF. secondary — Specifies whether the configuration was loaded from the secondary location specified in the BOF. tertiary — Specifies whether the configuration was loaded from the tertiary location specified in the BOF.
Last Booted Config File	Displays the URL and filename of the configuration file used for the most recent boot.
Last Boot Cfg Version	Displays the version of the configuration file used for the most recent boot.
Last Boot Config Header	Displays header information of the configuration file used for the most recent boot.
Last Boot Index Version	Displays the index version used in the most recent boot.
Last Boot Index Header	Displays the header information of the index used in the most recent boot.
Last Saved Config	Displays the filename of the last saved configuration.
Time Last Saved	Displays the time the configuration was most recently saved.

**Table 63 Show System Information Output Fields (Continued)**

Label	Description
Changes Since Last Save	Yes — Indicates that the configuration changed since the last save. No — Indicates that the configuration has not changed since the last save.
Time Last Modified	Displays the time of the last modification.
Max Cfg/BOF Backup Rev	Indicates the maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL — Indicates the location and name of the CLI script file executed following successful completion of the boot-up configuration file execution. N/A — Indicates that no CLI script file is executed.
Cfg-OK Script Status	Successful/Failed — Indicates the results from the execution of the CLI script file specified in the Cfg-OK Script location. Not used — Indicates that no CLI script file was executed.
Cfg-Fail Script	URL — Displays the location and name of the CLI script file executed following a failed boot-up configuration file execution. Not used — Indicates that no CLI script file was executed.
Cfg-Fail Script Status	Successful/Failed — Displays the results from the execution of the CLI script file specified in the Cfg-Fail Script location. Not used — Indicates that the CLI script file was executed.
Management IP address	Displays the Management IP address of the node.
DNS Server	Displays the DNS address of the node.
DNS Domain	Displays the DNS domain name of the node.
BOF Static Routes	To — Displays the static route destination. Next Hop — Displays the next hop IP address used to reach the destination. Metric — Displays the priority of this static route versus other static routes. None — Indicates that no static routes are configured.

# access-group

- Syntax** `access-group group-name`
- Context** `show>system>security`
- Description** This command displays access-group information.
- Output** The following is an example of access group information.

[Table 64](#) describes the access-group output fields.

## Sample Output

```
A:ALA-1# show system security access-group
=====
Access Groups
=====
group name      security  security  read      write      notify
                model    level    view      view      view
-----
snmp-ro         snmpv1   none     no-security      no-security
snmp-ro         snmpv2c  none     no-security      no-security
snmp-rw         snmpv1   none     no-security      no-security
snmp-rw         snmpv2c  none     no-security      no-security
snmp-rwa        snmpv1   none     iso              iso
snmp-rwa        snmpv2c  none     iso              iso
snmp-trap       snmpv1   none     no-security      iso
snmp-trap       snmpv2c  none     no-security      iso
-----
No. of Access Groups: 8
=====
A:ALA-1#

A:ALA-1# show system security access-group detail
=====
Access Groups
=====
group name      security  security  read      write      notify
                model    level    view      view      view
-----
snmp-ro         snmpv1   none     no-security      no-security
-----
No. of Access Groups:
...
=====
A:ALA-1#
```

**Table 64** Show System Security Access-Group Output Fields

Label	Description
Group name	The access group name.

**Table 64 Show System Security Access-Group Output Fields (Continued)**

Label	Description
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.

## authentication

- Syntax** `authentication [statistics]`
- Context** `show>system>security`
- Description** This command displays authentication information.
- Output** The following displays an example of authentication information.

[Table 65](#) describes the authentication output fields.

### Sample Output

```
A:ALA-49>show>system>security# authentication
=====
Authentication                               sequence : radius tacplus local
=====
type                status  timeout (secs)  retry count
server address
-----
radius              up      5              5
  10.10.10.103
radius              up      5              5
  10.10.10.1
radius              up      5              5
  10.10.10.2
radius              up      5              5
  10.10.10.3
-----
radius admin status : up
tacplus admin status : up
health check        : enabled (interval 30)
-----
No. of Servers: 4
=====
```



A:ALA-49>show>system>security#

**Table 65 Show Authentication Output Fields**

Label	Description
sequence	Displays the authentication order in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.
server address	Displays the address of the RADIUS, TACACS+, or local server.
status	Displays the status of the server.
type	Displays the type of server.
timeout (secs)	Displays the number of seconds the server will wait before timing out.
retry count	Displays the number of attempts to retry contacting the server.
radius admin status	Displays the administrative status of the RADIUS protocol operation.
tacplus admin status	Displays the administrative status of the TACACS+ protocol operation.
health check	Specifies whether the RADIUS and TACACS+ servers will be periodically monitored. Each server will be contacted every 30 seconds. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent.
No. of Servers	Displays the total number of servers configured.

## password-options

- Syntax** password-options
- Context** show>system>security
- Description** This command displays password options.
- Output** The following displays password option information.
- [Table 66](#) describes password-options output fields.

### Sample Output

```
A:ALA-48>show>system>security# password-options
=====
```

```

Password Options
=====
Password aging in days                : 365
Number of invalid attempts permitted per login : 5
Time in minutes per login attempt      : 5
Lockout period (when threshold breached) : 20
Authentication order                  : radius tacplus local
Configured complexity options         :
Minimum password length               : 8
=====
A:ALA-48>show>system>security#

```

**Table 66** Show Password-Options Output Fields

Label	Description
Password aging in days	Number of days a user password is valid before the user must change his password.
Number of invalid attempts permitted per login	Displays the maximum number of unsuccessful login attempts allowed for a user.
Time in minutes per login attempt	Displays the time in minutes that user is to be locked out.
Lockout period (when threshold breached)	Displays the number of minutes the user is locked out if the threshold of unsuccessful login attempts has exceeded.
Authentication order	Displays the most preferred method to authenticate and authorize a user.
Configured complexity options	Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the <b>authentication</b> section.
Minimum password length	Displays the minimum number of characters required in the password.

## per-peer-queuing

- Syntax** per-peer-queuing
- Context** show>system>security
- Description** This command displays the number of queues in use by the Qchip, which in turn is used by PPQ, CPM filter, SAP, and so on.
- Output** The following displays per peer queuing information.

[Table 67](#) describes the per-peer-queuing output fields.

### Sample Output

```
A:ALA-48>show>system>security# per-peer-queuing
=====
CPM Hardware Queuing
=====
Per Peer Queuing      : Enabled
Total Num of Queues   : 8192
Num of Queues In Use  : 0
=====
A:ALA-48>show>system>security#
```

**Table 67** Show per-peer-queuing Output Fields

Label	Description
Per Peer Queuing	Displays whether per-peer-queuing is enabled or disabled. When enabled, a peering session is established and the router will automatically allocate a separate CPM hardware queue for that peer. When disabled, no hardware queuing per peer occurs.
Total Num of Queues	Displays the total number of CPM hardware queues.
Num of Queues In Use	Displays the number of CPM hardware queues that are in use.

## profile

- Syntax** `profile [profile-name]`
- Context** `show>system>security`
- Description** This command displays user profiles for CLI command tree permissions.
- Parameters** *profile-name* — Specify the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names are listed.
- Output** The following displays an example of profile information.

[Table 68](#) describes the profile output fields.

### Sample Output

```
A:ALA-48>config>system>snmp# show system security profile
=====
User Profile
=====
User Profile : test
Def. Action  : none
-----
Entry       : 1
Description :
```

```
Match Command:
Action          : unknown
=====
User Profile   : default
Def. Action    : none
-----
Entry          : 10
Description    :
Match Command: exec
Action         : permit
-----
Entry          : 20
Description    :
Match Command: exit
Action         : permit
-----
Entry          : 30
Description    :
Match Command: help
Action         : permit
-----
...
-----
Entry          : 80
Description    :
Match Command: enable-admin
Action         : permit
=====

User Profile   : administrative
Def. Action    : permit-all
-----
Entry          : 10
Description    :
Match Command: configure system security
Action         : permit
-----
Entry          : 20
Description    :
Match Command: show system security
Action         : permit
=====
No. of profiles: 3
=====
A:ALA-48>config>system>snmp#
```

**Table 68**      **Show Profile Output Fields**

Label	Description
User Profile	default — Displays the action to be given to the user profile if none of the entries match the command.  administrative — Specifies the administrative state for this profile.

**Table 68 Show Profile Output Fields (Continued)**

Label	Description
Def. Action	<p>none — No action is given to the user profile when none of the entries match the command.</p> <p>permit-all — The action to be taken when an entry matches the command.</p>
Entry	10 - 80 — Displays an entry which represents the configuration for a system user.
Description	A text string describing the entry.
Match Command	<p>administrative — Enables the user to execute all commands.</p> <p>configure system security — Enables the user to execute the <b>config system security</b> command.</p> <p>enable-admin — Enables the user to enter a special administrative mode by entering the <b>enable-admin</b> command.</p> <p>exec — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console.</p> <p>exit — Enables the user to execute the <b>exit</b> command.</p> <p>help — Enables the user to execute the <b>help</b> command.</p> <p>logout — Enables the user to execute the <b>logout</b> command.</p> <p>password — Enables the user to execute the <b>password</b> command.</p> <p>show config — Enables the user to execute the <b>show config</b> command.</p> <p>show — Enables the user to execute the <b>show</b> command.</p> <p>show system security — Enables the user to execute the show system security command.</p>
Action	<p>permit — Enables the user access to all commands.</p> <p>deny-all — Denies the user access to all commands.</p>

## snmp

**Syntax** **snmp**

**Context** show>system>security

**Description** This command enables the context to show SNMP information.

community

- Syntax** `community community-string`
- Context** `show>system>security>snmp`
- Description** This command lists SNMP communities and characteristics. Including the *community-name* parameter modifies the output to include all details for the specified community, including the source IP address list and validation failure counters.
- Output** [Table 69](#) describes the community output fields.

Sample Output



**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-privatel         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          src-access-list  version  group name
-----
my-public2          r      no-security   my-list1         v1 v2c   snmp-ro
                                     my-list1         5
-----
=====
A:ALA-1#
```

**Table 69 Show Community Output Fields**

Label	Description
Community	Displays the community string name for SNMPv1 and SNMPv2c access only.
Access	Displays access information. r — The community string allows read-only access. rw — The community string allows read-write access. rwa — The community string allows read-write access. mgmt — The unique SNMP community string assigned to the management router. vpls-mgmt — The unique SNMP community string assigned for vpls management.
View	Displays the view name.
Version	Displays the SNMP version.
Group Name	Displays the access group name.
src-access-list	Displays 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	Displays the number of SNMP requests that have failed validation using this <b>community</b> .
No of Communities	Displays the total number of configured community strings.

## 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** The following example displays SR access list information.

[Table 70](#) describes the source access list output fields.

### Sample Output

```
A:ALA-1# show system security snmp src-access-list
=====
Source Access Lists
=====
```

```
List Name
  HostName                      Host Address
-----
L1
  H1                          10.100.100.1
  H2                          10.100.100.2
L2
  HA                          10.100.101.1
  HB                          10.100.101.2
-----
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                          10.100.100.1
  H2                          10.100.100.2
-----
Total Access Lists: 1
=====
A:ALA-1#
```

**Table 70**      **Show Source Access List Output Fields**

Label	Description
List Name	Displays the name of the <b>src-access-list</b> .
Host Name	Displays the name of the <b>src-host</b> .
Host Address	Displays the IP address of the <b>src-host</b> .
Total Access Lists	Displays the total number of source access lists.

ssh

- Syntax**      **ssh**
- Context**      show>system>security
- Description**      This command displays all the SSH sessions as well as the SSH status and fingerprint.
- Output**      The following shows an example of SSH information.  
[Table 71](#) describes SSH output fields.



### Sample output

```
A:ALA-7# show system security ssh
SSH is enabled
Key fingerprint: 34:00:f4:97:05:71:aa:b1:63:99:dc:17:11:73:43:83
=====
Connection Encryption Username
=====
192.168.0.0 3des admin
-----
Number of SSH sessions : 1
=====
A:ALA-7#

A:ALA-49>config>system>security# show system security ssh
SSH is disabled
A:ALA-49>config>system>security#
```

**Table 71** Show SSH Output Fields

Label	Description
SSH status	SSH is enabled — Displays that SSH server is enabled. SSH is disabled — Displays that SSH server is disabled.
Key fingerprint	The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected router(s) (remote client).
Encryption	des — Data encryption using a private (secret) key. 3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.
Username	The name of the user.
Number of SSH sessions	The total number of SSH sessions.

## user

- Syntax** `users [user-id] [detail]`
- Context** `show>system>security`
- Description** This command displays user information.
- Output** The following shows an example of user information.

[Table 72](#) describes user information output fields.

**Table 72 Show User Output Fields**

Label	Description
User ID	Displays the name of a system user.
Need New PWD	Yes — Specifies that the user must change his password at the next login. No — Specifies that the user is not forced to change his password at the next login.
User Permission	Console — Specifies whether the user is permitted console or Telnet access. FTP — Specifies whether the user is permitted FTP access. SNMP — Specifies whether the user is permitted SNMP access.
Password expires	Displays the date on which the current password expires.
Attempted logins	Displays the number of times the user has attempted to login irrespective of whether the login succeeded or failed.
Failed logins	Displays the number of unsuccessful login attempts.
Local Conf.	Y — Indicates that password authentication is based on the local password database. N — Indicates that 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** The following displays an example of system security views.

[Table 73](#) describes system security view output fields.

**Sample Output**

```
A:ALA-1# show system security view
=====
Views
=====
view name          oid tree          mask          permission
-----
iso                1                included
no-security        1                included
no-security        1.3.6.1.6.3      excluded
no-security        1.3.6.1.6.3.10.2.1 included
no-security        1.3.6.1.6.3.11.2.1 included
no-security        1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 6
=====
A:ALA-1#

A:ALA-1# show system security view no-security detail
=====
Views
=====
view name          oid tree          mask          permission
-----
no-security        1                included
no-security        1.3.6.1.6.3      excluded
no-security        1.3.6.1.6.3.10.2.1 included
no-security        1.3.6.1.6.3.11.2.1 included
no-security        1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 5
=====
no-security used in
=====
group name
-----
snmp-ro
snmp-rw
=====
A:ALA-1#
```

**Table 73** Show System Security View Output Fields

Label	Description
View name	Displays the name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.

**Table 73**      **Show System Security View Output Fields (Continued)**

Label	Description
OID tree	Displays the Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.
Mask	Displays the mask value and the mask type, along with the <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. Excluded — Specifies to exclude MIB subtree objects.
No. of Views	Displays the total number of configured views.
Group name	Displays the access group name.

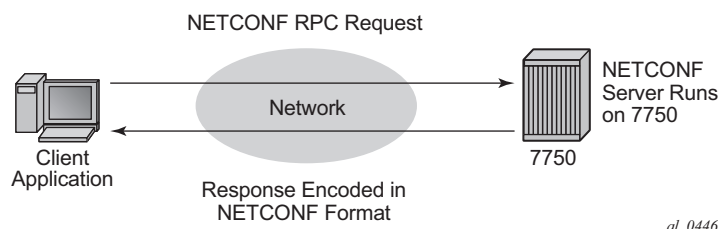
## 5 NETCONF

### 5.1 NETCONF Overview

NETCONF is a standardized IETF configuration management protocol published in RFC 6241, *Network Configuration Protocol (NETCONF)*. It is secure, connection-oriented, and runs on top of the SSHv2 transport protocol as specified in RFC 6242, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*. NETCONF is an XML-based protocol that can be used as an alternative to CLI or SNMP for managing an SR OS router.

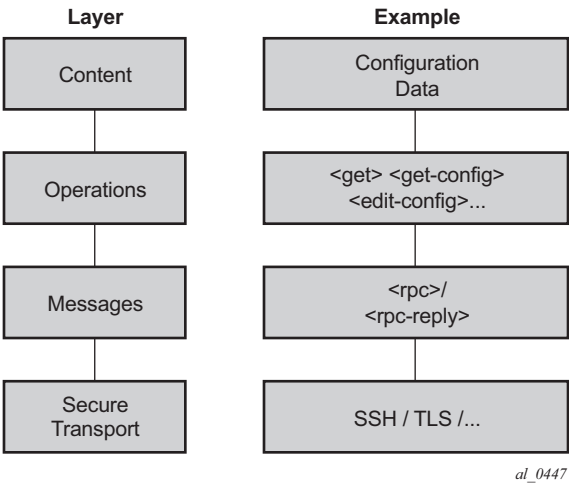
NETCONF uses RPC messaging for communication between a NETCONF client and the NETCONF server running on SR OS. An RPC message and configuration data is encapsulated within an XML document. These XML documents are exchanged between a NETCONF client and a NETCONF server in a request/response type of interaction. The SR OS NETCONF interface supports both configuration and retrieval of operational information. [Figure 15](#) shows a NETCONF RPC request.

**Figure 15 NETCONF RPC Request**



NETCONF can be conceptually partitioned into four layers as described in RFC 6241. [Figure 16](#) shows the NETCONF layers.

**Figure 16    NETCONF Layers (RFC 6241)**



---

## 5.2 NETCONF in SR OS

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

- Changing the configuration of the router (<edit-config> operation)
- Reading the configuration of the router (<get-config> operation, equivalent to the **info** command in the SR OS CLI)
- Reading operational status and data (and associated configuration information) (<get> operation, equivalent to the **show** commands in the SR OS CLI)
- Notifications on an SR OS router; equivalent to the SR OS log events.

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

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

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

The SR OS NETCONF server advertises the base:1.1 capability (in addition to base:1.0).

SR OS NETCONF supports both a CLI content layer and an XML-based content layer.

### 5.2.1 Transport and Sessions

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

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 SR OS. An access type 'netconf' is provided. For access to the Base-R13 SR OS YANG data models, both **console** and **netconf** access must be configured for the user. For access to the Nokia SR OS YANG data models, only **netconf** access is necessary.

Authentication via the local user database is supported for NETCONF users. NETCONF runs over SSH, and SSH supports RADIUS/TACACS+ user authentication. By adding "access netconf" under the default RADIUS/TACACS+ user-template, the NETCONF user is granted access.

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

Command authorization is supported for the Alcatel-Lucent Base-R13 SR OS YANG modules. Also, access to various CLI config and show commands (via the CLI content layer) is controlled through the profile assigned to the user that is used to authenticate the underlying SSH session.

Access to LI commands using the Alcatel-Lucent Base-R13 SR OS YANG modules is based on the **access li** configuration 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.

**Example** - A user request, with **show** command, that is not in the scope of the user's access profile.

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

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rpc-error>
    <error-type>application</error-type>
    <error-tag>operation-failed</error-tag>
    <error-severity>error</error-severity>
    <error-info>
      <err-element>cli-show</err-element>
    </error-info>
  </rpc-error>
</rpc-reply>
```



```

    </error-info>
    <error-message>
      command failed - 'show system security profile'
      MINOR: CLI Command not allowed for this user.
    </error-message>
  </rpc-error>
</rpc-reply>
]]>]]>

```

## 5.2.2 Datastores and URLs

SR OS supports the <running> datastore, the <candidate> datastore, the <startup> datastore, and <url>.



**Note:** <url> is not a datastore in itself.

Support for the <candidate> datastore capability is advertised via the SR OS NETCONF server <hello> as:

```
<capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
```

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

The <startup> datastore and <url> 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> as:

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

The <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> as:

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

The following examples show the format of each URL scheme:

- `<target><url>ftp://name:passwd@IP_ADDRESS/usr/myfiles/myfile.cfg</url></target>`
- `<target><url>tftp://name:passwd@IP_ADDRESS/usr/myfiles/myfile.cfg</url></target>`
- `<target><url>file:///cf3:/myfiles/myfile.cfg</url></target>`
- `<target><url>cf3:/myfiles/myfile.cfg</url></target>`



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

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

The BOF is not considered part of any configuration datastore.

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

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

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

Only the Nokia SR OS YANG modules can be used with the `<candidate>` datastore. The Alcatel-Lucent Base-R13 SR OS YANG modules are not applicable to the `<candidate>` datastore, but are applicable to the `<running>` datastore. All `<edit-config>` requests to the `<candidate>` datastore must use the `urn:nokia.com:sros:ns:yang:sr:conf` namespace.

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

## 5.2.3 NETCONF Operations and Capabilities

The following base protocol operations are supported:

- `<get>`
- `<get-config>`
- `<edit-config>`
- `<copy-config>` and `<delete-config>`
- `<lock>`
- `<unlock>`
- `<commit>`
- `<discard-changes>`
- `<validate>`
- `<close-session>`
- `<kill-session>`

The following optional capabilities from RFC 6241 are supported:

- Writable-Running Capability
- Candidate Configuration Capability
  - `<commit>` operation
  - `<discard-changes>` operation
- Confirmed Commit Capability
- Validate Capability
  - `<validate>` operation
- Distinct Startup Capability
- URL Capability

The following capability from RFC 6243 is supported:

- With-defaults Capability

The following capabilities from RFC 5277 are supported:

- notification capability
  - `<create-subscription>` operation
- interleave capability

The following capability from RFC 6022 is supported:

- ietf-network-monitoring capability
  - `<get-schema>` operation

The following capability from RFC 7950 is supported:

- yang-library capability
  - <get-schema> operation

One rpc request can only contain one operation.

Table 74 shows supported NETCONF operations.

**Table 74**      **NETCONF Operations**

Operation	Arguments
get-config	source [filter]
edit-config	target [default-operation] [test-option] [error-option] config
copy-config	target source
delete-config	target
lock	target
unlock	target
get	[filter]
close-session	n/a
kill-session	session-id
discard-changes	n/a
validate	source
commit	[confirmed] [confirm-timeout] [persist] [persist-id]
cancel-commit	[persist-id]
create-subscription	[stream] [startTime] [stopTime]
get-schema	identifier [version] [format]



**Note:** Bracketed arguments are optional.

### 5.2.3.1 <get>

The CLI content layer <get> operation is supported with both configuration and state data returned in a <get> reply. An XML content layer <get> operation, supported with both configurations and state data, being returned in a <get> reply as per the NOKIA SR OS YANG data models only.

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
```

```

10.23.63.5/32 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>
]]>]]>

```

### 5.2.3.2 <get-config>

The <get-config> operation returns non-default configuration by default for the Alcatel-Lucent Base-R13 SR OS YANG modules (the 'trim' mode as per RFC 6243).

The <get-config> operation returns data nodes that were set by a client to their default values for the NOKIA SR OS modules (the 'explicit' mode as per RFC 6243).

### 5.2.3.3 <edit-config>

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

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

The "replace" value for the "operation" parameter and the "default-operation" parameter is 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.

#### 5.2.3.4 <copy-config> and <delete-config>

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

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

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

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

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

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

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

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

- <url>
- <startup>

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

### 5.2.3.5 <lock>

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

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

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

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

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

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

- releases the lock
- discards the "uncommitted" changes (if any)



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



Timeouts of locks are not supported. No specific admin/tools commands are provided to release the lock without disconnecting the session that holds it, but the session that holds the lock can be administratively disconnected using a CLI command to release the lock.

Using a CLI **show** command, the operator can determine if the <running> datastore is locked, the <candidate> datastore is locked, or both are locked, and the session ID of the session that holds the lock; see the [NETCONF Show and Debug Command Reference](#).

From CLI, the operator can configure whether users that belong to a specific profile have permission to lock NETCONF sessions; see the [NETCONF Configuration Command Reference](#).

An active NETCONF session can be disconnected from the CLI using the session ID. The user can use the show command to find the NETCONF session ID then use the admin command to disconnect the NETCONF session using the session ID obtained from the show command. For details, see the [NETCONF Show and Debug Command Reference](#).

### 5.2.3.6 <unlock>

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

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

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

### 5.2.3.7 <commit>

The <commit> command has the following characteristics.

- It represents the equivalent of the CLI command **candidate commit**.
- When a <commit> operation fails, only the first error is returned.

- When SR OS cannot commit all the changes in the candidate datastore, SR OS keeps the <running> datastore unchanged.
- When a NETCONF session is disconnected (using Ctrl-c or <kill-session>) in the middle of a <commit> operation, SR OS keeps the running datastore unchanged.
- The persistency of changes made via a <commit> operation is operator-controlled. A copy of the running datastore to the startup datastore can be automatically performed after each successful <commit> operation. This behavior can be enabled or disabled through a CLI command.
- When some changes exist in the candidate datastore (prior to being committed to the running datastore), there are impacts to:
  - a CLI user trying to make immediate changes, as SR OS blocks all CLI immediate configurations
  - an SNMP set request, as SR OS blocks the request and returns an error
  - an <edit-config> to the running datastore, as SR OS blocks all <edit-config> requests to the running datastore and returns an error

The :confirmed-commit capability is advertised in the SR OS NETCONF server <hello> as:

```
<capability>urn:ietf:params:netconf:capability:confirmed-commit:1.1</capability>
```

The :confirmed-commit capability has the following characteristics:

- The capability is not advertised if the operator disables the candidate DS capability using the available SR OS CLI command.
- The parameters listed in [Table 75](#) are supported for the <commit> operation.

**Table 75** Parameters for a <commit> Operation

Parameter	Description
<confirmed>	This parameter indicates it is a confirmed <commit> operation.
<confirm-timeout>	This parameter specifies the timeout period for confirmed commit (in seconds). If unspecified, the confirmed commit timeout defaults to 600 seconds (10 minutes).

**Table 75 Parameters for a <commit> Operation (Continued)**

Parameter	Description
<persist>	This parameter configures the confirmed commit changes to survive a session termination. It sets a token on the ongoing confirmed commit. If <persist> is not given in the confirmed commit operation, any follow-up commit and the confirming commit must be issued on the same session that issued the confirmed commit. If <persist> is given in the confirmed commit operation, a follow-up commit and the confirming commit can be given on any session, but they must include a <persist-id> element with a value equal to the value of the <persist> element in the confirmed commit. The <persist> element can not be changed through a follow-up confirmed commit.
<persist-id>	This parameter issues a follow-up confirmed commit or the confirming commit from any session, using the same token from the <persist> element of the confirmed commit. The <persist-id> element cannot be changed through a follow-up confirmed commit.

- If <persist> was specified in the confirmed commit, the configuration changes are rolled back only if the timeout expires before receiving a confirming commit. The confirming commit has to include a <persist-id> tag with a value equal to the value of the <persist> tag that was in the confirmed commit.
- If the NETCONF session that initiated the confirmed commit is closed while waiting for the confirming commit (for example, disconnected), then SR OS restores the configuration to its state before the confirmed commit was issued. This is valid only if <persist> was not defined in the confirmed commit.
- If a follow-up confirmed commit is issued before the timer expires, the timer is reset to the new value.
- The confirming commit and the follow-up confirmed commit cannot introduce additional changes to the configuration.
- The <cancel-commit> operation is supported. It can cancel an ongoing confirmed commit (that is, cancel the timer and rollback the changes introduced with the confirmed commit).
- If the <persist> parameter is not given, the <cancel-commit> operation must be issued on the same session that issued the confirmed commit.

### 5.2.3.8 <discard-changes>

The <discard-changes> operation causes the <candidate> datastore to revert back to match the <running> datastore and releases the “implicit” lock. From the CLI, the operator can do the equivalent of a <discard-changes> operation which releases the implicit lock as well (see [NETCONF Admin Command Reference](#)).

### 5.2.3.9 <validate>

The validate capability is supported in the following ways:

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

### 5.2.3.10 <get-schema>

A <get-schema> operation is supported for explicit schema retrieval via NETCONF. See [NETCONF Monitoring](#) for more information.

## 5.2.4 Data Model, Datastore and Operation Combinations

[Table 76](#) shows the which operations are supported by data model and datastore combination.

**Table 76 Data Model, Datastore and Operation Combinations**

Operation	R13 Modules		Nokia Modules	
	<running>	<candidate>	<running>	<candidate>
<edit-config>	supported	not supported	not supported	supported
<get-config>	supported	not supported	supported	supported
<get>*	not supported		retrieves both configuration and state data (XML format only)	

\* - Note that the <running> or <candidate> datastores are not applicable for a <get> operation.

A <get> operation can retrieve CLI content layer state data.

## 5.2.5 General NETCONF Behavior

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

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

If an invalid namespace is specified within the client's hello message, no error will be returned as the NETCONF server is still waiting for the client to send a valid <hello/>. Further NETCONF requests (without sending a proper hello message) even though correct, SR OS returns an error in that case indicating that "Common base capability not found."

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

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

In the <rpc> element, prefixes are accepted and have to be specified with a valid URI. If an incorrect URI is declared with a prefix, then SR OS detects the invalid URI and sends an <rpc-error> response.

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

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

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

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

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

Or:

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

- The NETCONF client can declare those two namespaces with prefixes at the <rpc> tag itself and use the corresponding prefixes later in the request message's <configure/> block.
- SR OS returns an error if the request contains one or more incorrect namespaces.

### Example 1 — the standard NETCONF namespace

"urn:ietf:params:xml:ns:netconf:base:1.0" is used more than once in the <rpc> element:

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

Reply (no error message):

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

```

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

```

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

```

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

```

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

```

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

```

**Example 3** — an invalid NETCONF namespace is declared in the <rpc> element:

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

**Reply (SR OS returns an error):**

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

**Example 4** — a non-default NETCONF namespace/prefix declared in any child tag overrides the one declared under 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 xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
        <router>
          <interface xmlns:alu="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
            <alu:interface-name>"system"</alu:interface-name>
          </interface>
        </router>
      </configure>
    </filter>
  </get-config>
</rpc>
```



```

        </configure>
    </filter>
</get-config>
</rpc>
]]>]]>

```

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

```

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

```

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

#### Example 5 — Chunked message:

```

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

```

#### Example 6 — Chunked message:

```

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

```

```

<system>
<netconf>
</netconf>
</system>
##43
</configure>
</filter>
</get-config>
</rpc>
##

```

Handling of default data (for example, “info” vs “info detail”) uses the mechanisms detailed in RFC 6243. The SR OS NETCONF server supports the 'trim' method as the default for the Alcatel-Lucent Base-R13 SR OS YANG modules. It supports the 'explicit' method as the default for the NOKIA SR OS Yang modules and also supports the 'report-all' method.

The advertised capability changes depending on which YANG modules are enabled or disabled in SR OS:

- When base-r13 modules are enabled and all other modules are disabled, the following capability is advertised:  
`<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=trim&also-supported=report-all</capability>`
- For all the other scenarios, the following capability is advertised:  
`<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=explicit&also-supported=report-all</capability>`

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

The set of supported actions are as follows:

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

#### Example 7 — Two rollback items with responses:

```

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

```

```

    </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
-     service
-         vpls "99" customer 1 create
-             shutdown
-             stp
-             shutdown
-         exit
-     exit
-     exit
-     exit
-     exit
-----
Finished in 0.350 s
        </response>
    </item>
</cli-action>
</data>
</rpc-reply>
]]>]]>

```

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

```

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

```

### Reply:

```

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

```

### Example 9 — Error processing the request:

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

### Reply:

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

```

        </item>
      </cli-action>
    </data>
  </rpc-reply>
]]>]]>

```

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

```

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

```

Reply:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="104" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data xmlns="urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-r13">
    <cli-action>
      <item>
        <admin>rollback compare active-cfg to 1</admin>
        <response>
          0.170 s
          1.350 s
          -----
          configure
            router
            -   mpls
            -   shutdown
            -   interface "system"
            -     no shutdown
            -   exit
            -   exit
            -   rsvp
            -     shutdown
            -     interface "system"
            -       no shutdown
            -     exit
            -   exit
            exit
            exit
          -----
          Finished in 1.640 s
        </response>
      </item>
      <item>
        <admin>rollback compare 1 to xyz</admin>
        <response>
        </response>
        <rpc-error>

```

```

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

A **debug system netconf info** command can be used to dump NETCONF debug message streams. For further details and an example, see the [NETCONF Show and Debug Command Reference](#).

## 5.3 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@IP_ADDRESS -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</
    capability>
    <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:confirmed-commit:1.1</
    capability>
    <capability>urn:ietf:params:netconf:capability:notification:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:interleave:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
    <capability>urn:ietf:params:netconf:capability:startup:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:url:1.0?scheme=ftp,tftp,file<
    /capability>
    <capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-
    mode=explicit&also-supported=report-all</capability>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0?module=ietf-
    netconf&revision=2011-06-01&features=writable-
    running,validate,startup,url&deviations=alu-netconf-deviations-r13</
    capability>
    <capability>urn:alcatel-lucent.com:sros:ns:yang:netconf-deviations-
    r13?module=alu-netconf-deviations-r13&revision=2015-01-23</capability>
    <capability>urn:alcatel-lucent.com:sros:ns:yang:cli-content-layer-
    r13?module=alu-cli-content-layer-r13&revision=2015-01-23</capability>
    <capability>urn:alcatel-lucent.com:sros:ns:yang:conf-r13?module=alu-conf-
    r13&revision=2018-03-15</capability>
    ...
  </capabilities>
  <session-id>69</session-id>
</hello>
]]>]]>
```

A NETCONF client can reply with a hello message like the following:

```
<?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>
      </capabilities>
</hello>
]]>]]>
```

## 5.4 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.

### 5.4.1 <get> with XML Content Layer

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

**Example 1:** The <configure> tag contains a namespace

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

Reply: no errors

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

```

    </data>
  </rpc-reply>
]]>]]>

```

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

```

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

```

### Reply: SR OS errors

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rpc-error>
    <error-type>protocol</error-type>
    <error-tag>unknown-element</error-tag>
    <error-severity>error</error-severity>
    <error-info>
      <bad-element>configure</bad-element>
    </error-info>
    <error-message>
      Element is not valid in the specified context.
    </error-message>
  </rpc-error>
</rpc-reply>
]]>]]>

```

### Example 3: The <state> tag contains a namespace

```

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

```

### Reply: No errors

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <state xmlns="urn:nokia.com:sros:ns:yang:sr:state">

```

```
...
...
    </state>
  </data>
</rpc-reply>
]]>]]>
```

#### Example 4: The <state> tag does not contain a namespace

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

#### Reply: SR OS errors

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rpc-error>
    <error-type>protocol</error-type>
    <error-tag>bad-element</error-tag>
    <error-severity>error</error-severity>
    <error-info>
      <bad-element>state</bad-element>
    </error-info>
    <error-message>
      Element is not valid in the specified context.
    </error-message>
  </rpc-error>
</rpc-reply>
]]>]]>
```

## 5.4.2 <edit-config> with XML Content Layer

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

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

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

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

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

**Reply:** with SR OS errors

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

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

- The first NETCONF <edit-config> on a <candidate> datastore triggers the “implicit” lock
- The completion of a NETCONF <commit> releases the “implicit” lock
- A CLI **admin** command can release the “implicit” lock. For more information, see [5.11](#)
- The NETCONF <discard-changes> command is supported in SR OS which releases the “implicit” lock as well

The following scenarios are impacted when an “implicit” lock is taking place:

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

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

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

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

The supported <edit-config> operation attribute values are listed in [Table 77](#).

**Table 77      <edit-config> Operation Attribute Values**

Command	Notes
urn:alcatel-lucent.com:sros:ns:yang:conf-*-r13 namespace Alcatel-Lucent Base-R13 SR OS YANG modules	

**Table 77** **<edit-config> Operation Attribute Values (Continued)**

Command	Notes
merge (Base-R13 SR OS modules)	<ul style="list-style-type: none"> <li>For a merge operation, the operations and tags specified in an &lt;edit-config&gt; request are order-aware and order-dependent, and the sequence of merge operations must follow the required sequence of the equivalent CLI commands. The &lt;edit-config&gt; request is processed and executed in a top-down order. The same leaf can be enabled and disabled multiple times in the request and the final result is whatever was last specified for that leaf in the &lt;edit-config&gt; request.</li> </ul>
remove (Base-R13 SR OS modules)	<ul style="list-style-type: none"> <li>A &lt;remove&gt; operation is not supported for boolean leaves. For example, any of the following example commands will return an error: <ul style="list-style-type: none"> <li>&lt;shutdown operation="remove"/&gt;</li> <li>&lt;shutdown operation="remove"&gt;false&lt;/shutdown&gt;</li> <li>&lt;interface operation="remove"&gt; <ul style="list-style-type: none"> <li>&lt;interface-name&gt;abc&lt;/interface-name&gt;</li> <li>&lt;shutdown&gt;true&lt;/shutdown&gt;</li> </ul> &lt;/interface&gt; </li> </ul> (For this last case &lt;shutdown operation="merge"&gt;true&lt;/shutdown&gt; could be used instead to make the request valid.) </li> <li>A &lt;remove&gt; operation is the equivalent of <b>no command</b> in the CLI. This <b>no command</b> is applied whether the default for <i>command</i> is enabled (<i>command</i>), disabled (<b>no command</b>), or a specific value. The &lt;remove&gt; operation is not aware of the default value of the object or leaf being removed.</li> <li>A &lt;remove&gt; operation for a leaf where the request also specifies a value for the leaf, will result in an error.</li> </ul>

**Table 77**      **<edit-config> Operation Attribute Values (Continued)**

Command	Notes
delete (Base-R13 SR OS modules)	<ul style="list-style-type: none"> <li>• A &lt;delete&gt; operation for a leaf or a presence container will not return an error if the item is already deleted.</li> <li>• An error is returned if attempting to delete a list node that does not exist.</li> <li>• A &lt;delete&gt; operation for a container without presence will return an error.</li> <li>• A &lt;delete&gt; operation is not supported for boolean leaves. For example, any of the following example commands will return an error: <ul style="list-style-type: none"> <li>– &lt;shutdown operation="delete"/&gt;</li> <li>– &lt;shutdown operation="delete"&gt;false&lt;/shutdown&gt;</li> <li>– &lt;interface operation="delete"&gt; <ul style="list-style-type: none"> <li>&lt;interface-name&gt;abc&lt;/interface-name&gt;</li> <li>&lt;shutdown&gt;true&lt;/shutdown&gt;</li> </ul> </li> </ul> </li> </ul> <p>(For this last case &lt;shutdown operation="merge"&gt;true&lt;/shutdown&gt; could be used instead to make the request valid.)</p> <ul style="list-style-type: none"> <li>• A &lt;delete&gt; operation is the equivalent of <b>no command</b> in the CLI. This <b>no command</b> is applied whether the default for <i>command</i> is enabled (<i>command</i>), disabled (<b>no command</b>), or a specific value. The &lt;delete&gt; operation is not aware of the default value of the object/leaf being deleted.</li> <li>• A &lt;delete&gt; operation on a node will ignore any values provided for that node (it will not check if that value is configured or valid), and it will ignore any data below that node (it will not check if that data exists or is valid).</li> </ul>
create (Base-R13 SR OS modules)	<ul style="list-style-type: none"> <li>• A &lt;create&gt; operation for a leaf or a presence container will not return an error if the item is being set to the same value.</li> <li>• An error is returned if attempting to create a list node that already exists.</li> <li>• A &lt;create&gt; operation for a container without presence will result in an "OK" response (no error) but will be silently ignored.</li> <li>• For a &lt;create&gt; operation, the operations and tags specified in an &lt;edit-config&gt; request are order-aware and order-dependent, and the sequence of create operations must follow the required sequence of the equivalent CLI commands. The &lt;edit-config&gt; request is processed and executed in a top-down order. The same leaf can be enabled and disabled multiple times in the request and the final result is whatever was last specified for that leaf in the &lt;edit-config&gt; request.</li> </ul>
replace (Base-R13 SR OS modules)	<ul style="list-style-type: none"> <li>• not supported</li> </ul>
<b>urn:nokia.com:sros:ns:yang:sr:conf namespace</b> Nokia SR OS YANG modules	



**Table 77**      **<edit-config> Operation Attribute Values (Continued)**

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

**Table 77**      **<edit-config> Operation Attribute Values (Continued)**

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

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

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

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

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

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

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



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

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

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

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

1. Create

Create/Merge: SR OS processes request (request succeeds/fails based on operation's behavior)

Delete/Remove: SR OS returns an error

2. Merge

Create/Merge/Delete/Remove: SR OS processes request (request succeeds/fails based on operation's behavior)

3. Delete/Remove

Create/Merge: SR OS returns an error

Delete/Remove: SR OS processes request (request succeeds/fails based on operation's behavior)

### 5.4.3 <get-config> with XML Content Layer

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

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

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

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

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

The following applies to the urn:alcatel-lucent.com:sros:ns:yang:conf-\*-r13 namespace (the Alcatel-Lucent Base-R13 SR OS YANG modules):

- <get-config> requests that specify a non-existing 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.

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

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

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

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

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

```

        <system>
          <security>
            <cpm-filter>
              <ipv6-filter>
                </ipv6-filter>
              </cpm-filter>
            </security>
          </system>
        </configure>
      </filter>
      <with-defaults xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-with-defaults">
        report-all
      </with-defaults>
    </get-config>
  </rpc>
]>]]>

```

**Reply:** returns even attributes with default values

```

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

```

### Example 2: without using <with-defaults>

```

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

```

```
</get-config>
</rpc>
]]>]]>
```

**Reply:** Attributes with default values are not returned

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

Subtree filtering is supported for XML content layer <get-config> and <get> requests.

The subtree filtering behavior is as follows.

- Containment nodes are supported (as per section 6.2.3 of RFC 6241). Nodes that contain children nodes (containers) can be used for subtree filtering.

**Example 3 — A containment node:**

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

- Attribute match expressions (section 6.2.2 of RFC 6241) are not supported.
- Selection nodes are supported (as per section 6.2.4 of RFC 6241). Empty leaf nodes and list name nodes can be used as selection nodes. A selection node that is a list and does not have a key specified is supported.

**Example 4 — List without keys specified:**

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

**Example 5 — List with a non-key leaf specified as a selection node (keys should be returned as well).**

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

- Content match nodes are supported (as per section 6.2.5 of RFC 6241). Content match nodes that are leafs but not keys are also supported.

**Example 6 — A non key leaf is specified as a content match node.**

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



```

        </router>
      </configure>
    </filter>
  </get-config>
</rpc>
]]>]]>

```

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 7 — Content match node on a list key.

```

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

```

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

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

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

For example:

```

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

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

```

```

    </get-config>
  </rpc>
]>]]>

```

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

For example:

```

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

```

```

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

```

## 5.4.4 XML Content Layer Examples

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

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

```

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

```

Reply:

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

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

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

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <configure xmlns="urn:nokia.com:sros:ns:yang:sr:conf">
      <system>
        <contact>tester</contact>
        <name>r2-node</name>
        <location>over-here</location>
        <lldp>
          <shutdown>false</shutdown>
        </lldp>
        ...
        ...
      </system>
      <qos>
```

```

        <sap-ingress>
          <policy-id>1</policy-id>
          <policy-name>default</policy-name>
          <description>Default SAP ingress QoS policy.</description>
          <sub-insert-shared-pccrule>
          </sub-insert-shared-pccrule>
          <dynamic-policer>
            <range>
            </range>
            <parent>
            </parent>
          </dynamic-policer>
          <mac-criteria>
          </mac-criteria>
          <ip-criteria>
          </ip-criteria>
          <ipv6-criteria>
          </ipv6-criteria>
        </sap-ingress>
      </sap-egress>
    </qos>
  <log>
    <route-preference>
    </route-preference>
    <app-route-notifications>
    </app-route-notifications>
    <event-control>
      <application-id>1</application-id>
      <event-number>4401</event-number>
      <severity-level>major</severity-level>
      <throttle>true</throttle>
    </event-control>
  </log>
</configure>
</data>
</rpc-reply>
]]>]]>

```

The following is an example of an `<edit-config>` request on the `<running>` datastore to create a basic VPRN service:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <configure xmlns="urn:alcatel-lucent.com:sros:ns:yang:conf-r13">
        <service>
          <vprn operation="create">
            <service-id>200</service-id>
            <customer>1</customer>
          </vprn>
        </service>
      </configure>
    </config>
  </edit-config>
</rpc>

```

```

        </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>
]]>]]>

```

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

```

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

```

#### Reply:

```

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

```

## 5.5 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, *With-defaults capability for NETCONF*) 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].

## 5.5.1 CLI Content Layer Examples

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

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



**Note:** The **exit all** command is not required at the beginning of the CLI block; it is automatically assumed by the 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>
]]>]]>
```

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

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

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

**Reply:**

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

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





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

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

Reply:

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

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

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

```

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

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

```

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

```

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

```

```

        </filter>
      </get>
    </rpc>
  ]]>]]>

```

### Reply:

```

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

```

#### SSH Server

```

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

SSH Protocol Version 1    : Disabled

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

```

```

-----
Connection                               Username
  Version Cipher                         ServerName  Status
-----
10.121.143.254                           admin
      2          aes128-cbc                netconf    connected
-----

```

Number of SSH sessions : 1

```

=====
      </response>
    </item>
  </oper-data-format-cli-block>
</data>
</rpc-reply>
]]>]]>

```

## 5.6 NETCONF Notifications

NETCONF notifications support is a standard IETF asynchronous notification delivery service for the Network Configuration protocol (NETCONF) that is published in RFC 5277.

The :notification capability and the :interleave capability are advertised in the SR OS NETCONF server <hello> as:

```
<capability>urn:ietf:params:netconf:capability:notification:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:interleave:1.0</capability>
```

The following are characteristics of the NETCONF notifications capabilities supported in SR OS:

- The :notification capability indicates that the SR OS NETCONF server can process a subscription and send event notifications to the NETCONF client.
- The :interleave capability indicates that the SR OS NETCONF server supports receiving, processing, and responding to NETCONF requests on the same NETCONF session that has an active notification subscription.
- A NETCONF client needs to maintain an open NETCONF session with the NETCONF server in order to receive NETCONF notifications (that is, connection oriented).
- A NETCONF client can send a <create-subscription> RPC to the SR OS NETCONF server to start receiving notification messages.
- If the SR OS NETCONF server can satisfy the request, SR OS sends an <OK> element within the <rpc-reply>.
- If the SR OS NETCONF server cannot satisfy the request, SR OS sends an <rpc-error> element within the <rpc-reply>.
- Subscriptions are non persistent and their lifetime is defined by their NETCONF session (not maintained with a router reboot).
- An optional parameter that can be defined for a <create-subscription> RPC is: [stream]. The following are characteristics of the [stream] parameter:
  - An event stream is a set of event notifications matching a specified forwarding criteria and available to the NETCONF clients for subscription.
  - A NETCONF session can subscribe to only one stream at a time.
  - One stream can be subscribed-to by many NETCONF sessions.
  - The SR OS NETCONF server maintains one or more event streams.
  - SR OS uses the SR OS event reporting framework for NETCONF notifications.

- A log-id can be configured to be a NETCONF stream. A “netconf-stream” exists per a log-id. It is used to assign a NETCONF “stream” name with a log-id. A “netconf-stream” is unique per SR OS device. It must be configured with “to netconf” for subscriptions to be accepted. If a “netconf-stream” is changed, active subscriptions to the changed NETCONF stream name are terminated by SR OS.
- There is one pre-configured stream with the “netconf-stream” set to “NETCONF”, that is, log-id 101. It is used by default if the [stream] parameter is not specified. The pre-configured stream is modifiable but not deletable.
- Other streams can be configured via NETCONF or CLI. These streams are user-configured, which means that they are modifiable and can be deleted. A user-configured stream’s “netconf-stream” cannot be set to “NETCONF” as “NETCONF” is reserved for the pre-configured stream (that is, log-id 101).
- When a NETCONF client tries to subscribe to the SNMP log-id or a non-configured log-id, SR OS returns an error.
- SR OS supports a maximum number of 64 concurrent subscriptions to all streams.
- Notifications can be filtered out using a log-id’s “filter” or using base-op for create-subscriptions rpc.
- After the NETCONF server receives an SR OS event through a stream, a <notification> element is ready to be sent to all NETCONF sessions subscribed to that stream as per their filters.
- SR OS supports the following NETCONF notifications:
  - **sros-config-change-event**: sent with every configuration change; that is, any new, deleted, or modified configuration
  - **sros-state-change-event**: sent with every state change
  - **sros-command-accounting-event**: sent to keep track of which user did what activity on the SR OS device
  - **sros-log-generic-event**: contains the rest of the SR OS log events (except for the LI ones)
  - **netconf-config-change**: A notification based on the model-driven configuration change log event (the “mdConfigChange” log event). It is sent upon any configuration change happening by a model-driven management interface to the running datastore in the system. By default, this notification is disabled as the log event is also disabled by default. The notification is using the standard notification: netconf-config-change (as per RFC6470) augmented with a value leaf.

Bundling of a group of edits is allowed in a single **netconf-config-change** notification. That is, one notification can include many configuration changes.

The following example shows a `<create-subscription>` operation and the received response:

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

The following is an example for a `sros-config-change-event` notification:

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2017-06-12T09:12:43.376Z</eventTime>
  <sros-config-change-event xmlns="urn:nokia.com:sros:ns:yang:sr:notifications">
    <sequence-number>8447</sequence-number>
    <severity>warning</severity>
    <application>system</application>
    <event-id>2008</event-id>
    <event-name>tmnxConfigDelete</event-name>
    <router-name>Base</router-name>
    <subject>LDP</subject>
    <message>vRtrLdpNgSessionTable: Virtual Router 1, Peer 2.2.2.2:0. managed ob
ject deleted</message>
    <event-params>
      <tmnxNotifyRow>vRtrLdpNgSessState.1.1.6.2.2.2.0.0</tmnxNotifyRow>
      <tmnxNotifyEntryOID>vRtrLdpNgSessionEntry</tmnxNotifyEntryOID>
      <tmnxNotifyObjectName>vRtrLdpNgSessionTable: Virtual Router 1, Peer 2.2.
2.2:0.</tmnxNotifyObjectName>
    </event-params>
  </sros-config-change-event>
</notification>
```

The following is an example for a `sros-state-change-event` notification:

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2017-06-12T09:16:36.781Z</eventTime>
  <sros-state-change-event xmlns="urn:nokia.com:sros:ns:yang:sr:notifications">
    <sequence-number>8460</sequence-number>
    <severity>warning</severity>
    <application>system</application>
    <event-id>2009</event-id>
    <event-name>tmnxStateChange</event-name>
```

```

    <router-name>Base</router-name>
    <subject>LDP</subject>
    <message>Status of vRtrLdpNgSessionTable: Virtual Router 1, Peer 2.2.2.2:0.
changed administrative state: inService, operational state: inService</message>
    <event-params>
      <tmnxNotifyRow>vRtrLdpNgSessState.1.1.6.2.2.2.2.0.0</tmnxNotifyRow>
      <tmnxNotifyRowAdminState>inService</tmnxNotifyRowAdminState>
      <tmnxNotifyRowOperState>inService</tmnxNotifyRowOperState>
      <tmnxNotifyEntryOID>vRtrLdpNgSessionEntry</tmnxNotifyEntryOID>
      <tmnxNotifyObjectName>vRtrLdpNgSessionTable: Virtual Router 1, Peer 2.2.
2.2:0.</tmnxNotifyObjectName>
    </event-params>
  </sros-state-change-event>
</notification>

```

The following is an example for a sros-cli-accounting-event notification:

```

<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2017-06-12T09:11:45.476Z</eventTime>
  <sros-command-accounting-
event xmlns="urn:nokia.com:sros:ns:yang:sr:notifications">
    <sequence-number>8462</sequence-number>
    <severity>minor</severity>
    <application>user</application>
    <event-id>2011</event-id>
    <event-name>cli_config_io</event-name>
    <router-name>Base</router-name>
    <subject>admin</subject>
    <message>User from CONSOLE: Dut-C>config>log>log-id# /
configure router interface "toDutB_214" </message>
    <event-params>
      <srcAddr>CONSOLE</srcAddr>
      <prompt>Dut-C>config>log>log-id# </prompt>
      <message>/configure router interface "toDutB_214" </message>
    </event-params>
  </sros-command-accounting-event>
</notification>

```

The following is an example for a sros-log-generic-event notification:

```

<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2017-06-12T09:12:42.344Z</eventTime>
  <sros-log-generic-event xmlns="urn:nokia.com:sros:ns:yang:sr:notifications">
    <sequence-number>8443</sequence-number>
    <severity>warning</severity>
    <application>ospf</application>
    <event-id>2047</event-id>
    <event-name>tmnxOspfNgIfStateChange</event-name>
    <router-name>Base</router-name>
    <subject>VR: 1 OSPFv2 (0) </subject>
    <message>LCL_RTR_ID 1.1.1.1: Interface toDutB_214 state changed to down (eve
nt IF_DOWN) </message>
    <event-params>
      <vRtrID>1</vRtrID>
      <tmnxOspfVersion>version2</tmnxOspfVersion>
      <tmnxOspfInstance>0</tmnxOspfInstance>
      <tmnxOspfRouterId>16843009</tmnxOspfRouterId>

```

```

        <tmnxOspfNgIfIndex>0x00000007</tmnxOspfNgIfIndex>
        <tmnxOspfNgIfInstId>0</tmnxOspfNgIfInstId>
        <tmnxOspfNgIfAreaId>0</tmnxOspfNgIfAreaId>
        <tmnxOspfNgIfState>down</tmnxOspfNgIfState>
        <tmnxOspfIfIpAddress>toDutB_214</tmnxOspfIfIpAddress>
        <tmnxOspfIfEvent>IF_DOWN</tmnxOspfIfEvent>
        <ospfRouterIdIpAddress>1.1.1.1</ospfRouterIdIpAddress>
    </event-params>
</sros-log-generic-event>
</notification>

```

The following is an example for a netconf-config-change notification:

```

<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0"> <eventTime>20
16-01-01T19:17:33Z</eventTime>
<netconf-config-change
  xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-notifications"
  xmlns:notif="urn:nokia.com:sros:ns:yang:sr:notifications"
  xmlns:sros="urn:nokia.com:sros:ns:yang:sr:conf">
  <changed-by>
    <username>user_name</username>
    <session-id>8</session-id>
    <source-host>138.192.72.45</remote-host>
  </changed-by>
  <datastore>running</datastore>
  <edit>
    <target>/config/service/epipe[serviceId=1]</target>
    <operation>create</operation>
    <notif:value>anyValue</notif:value>
  </edit>
</netconf-config-change>
</notification>

```

In a <create-subscription>, a <filter> is an optional argument that is not supported by SR OS.

In a <create-subscription>, a <startTime> is an optional argument. This argument triggers the starting time of a replay. If it is not present, the subscription cannot be used to replay. A <startTime> cannot specify a time that is later than the current time (that is, in the future). SR OS supports timezones.

In a <create-subscription>, a <stopTime> is another optional argument. If this argument is not present, notifications continue to be sent until the subscription is terminated. A <stopTime> can specify a time that is later than the current time (that is, in the future). SR OS supports timezones.

A replay buffer is maintained by the SR OS server (per-stream) and sorted by the order they were initially sent out (that is, by sequence-id, and not by timestamps).

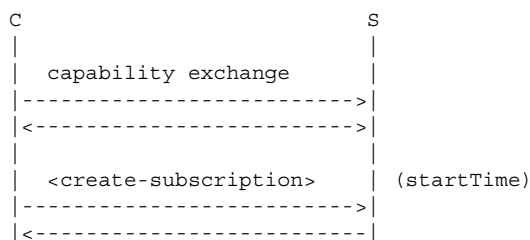
- A replay request from the client causes stored events to be sent to the client for the specified time interval.

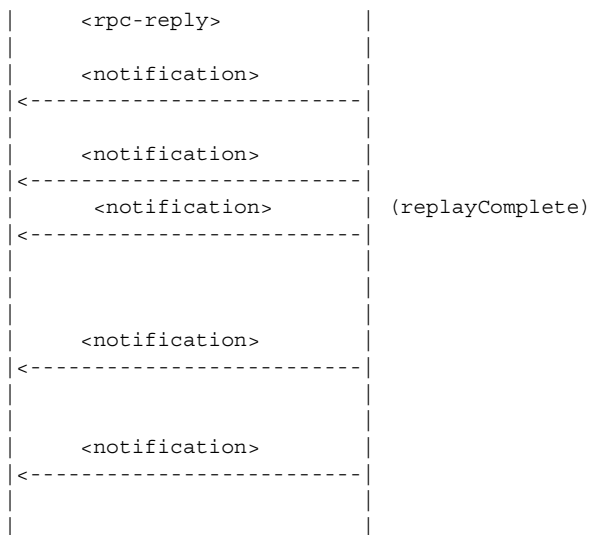


- A stream that supports replay is not expected to have an unlimited supply of saved notifications available to accommodate any replay request.
- The <startTime> and <stopTime> arguments are to specify when collections begin and end, respectively.
- A <replayComplete> notification is sent to indicate that all the replay notifications have been sent.
  - If a <stopTime> was specified, then the session then becomes a normal NETCONF session, and the NETCONF server then accepts <rpc> operations. A <notificationComplete> notification is expected after the <replayComplete> if the <stopTime> was specified. The following is an example of a session with a <stopTime> specified:



- If <stopTime> was not specified, the session will continue to send notifications as they arise in the system. The following is an example of a session without a <stopTime> specified:





- If neither `<startTime>` and `<stopTime>` arguments are present, no replay is present and notifications continue to be sent until the subscription is terminated.

## 5.7 NETCONF Monitoring

The `:ietf-netconf-monitoring` capability is advertised in the SR OS NETCONF server `<hello>` as:

```
<capability>urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring</capability>
```

The advertised capability provides information about the schemas supported by SR OS which allows a NETCONF client to query and retrieve schema information from the SR OS NETCONF server.

SR OS supports the `/netconf-state/schemas` subtree only from the YANG model that is used to monitor the NETCONF protocol as per RFC6022 (that is, `:ietf-netconf-monitoring` capability).

SR OS links retrieving the supported schemas to all the CLI commands that are used to enable and disable the YANG modules. The following are examples:

- A `/netconf-state/schemas` path returns all supported Nokia models (modules and sub-modules) when the **nokia-modules** parameter is set to **true**.
- A `/netconf-state/schemas` path returns the supported combined Nokia (flat) models when the **nokia-combined-modules** parameter is set to **true**.
- A `/netconf-state/schemas` path returns the ietf modules (for example, `ietf-inet-types` or `ietf-yang-types`) and the Nokia types in the returned list of schemas when either the **nokia-modules** or **nokia-combined-modules** is enabled.
- The ALU base-r13 YANG is not returned (regardless if its command was set to **true** or **false**).

The following example shows a request and the received response:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter>
      <netconf-state xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
        <schemas/>
      </netconf-state>
    </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>
    <netconf-state xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
```

```

    <schemas>
      <schema>
        <identifier>nokia-conf</identifier>
        <version>2016-07-06</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:conf</namespace>
        <location>NETCONF</location>
      </schema>
      <schema>
        <identifier>nokia-conf-aa-group</identifier>
        <version>2018-09-14</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:conf</namespace>
        <location>NETCONF</location>
      </schema>
      <schema>
        <identifier>nokia-conf-aaa</identifier>
        <version>2018-08-27</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:conf</namespace>
        <location>NETCONF</location>
      </schema>
      ...
      ...
      <schema>
        <identifier>nokia-state</identifier>
        <version>2016-07-06</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:state</namespace>
        <location>NETCONF</location>
      </schema>
      <schema>
        <identifier>nokia-state-aa-group</identifier>
        <version>2018-09-14</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:state</namespace>
        <location>NETCONF</location>
      </schema>
      <schema>
        <identifier>nokia-state-aaa</identifier>
        <version>2018-08-27</version>
        <format>yang</format>
        <namespace>urn:nokia.com:sros:ns:yang:sr:state</namespace>
        <location>NETCONF</location>
      </schema>
      ...
      ...
    </schemas>
  </state>
</data>
</rpc-reply>

```

A `<get-schema>` operation is supported for explicit schema retrieval using NETCONF (YANG data models' discovery and download as per RFC6022). The following parameters are supported:

- **identifier**: A mandatory string. Specifies an identifier for the schema list entry (YANG file). It can be the name of a module or a submodule.
- **version**: An optional string. Specifies a version of the schema requested (for example, YANG file). It represents the most recent YANG **revision** statement in a module or submodule. Empty string if no **revision** statement is present. As multiple versions may be supported by the NETCONF server, each version must be reported individually in the schema list (it can have same identifier but different versions).
- **format**: An optional string. Specifies the data modeling language that the schema is written in. Default value is 'yang' when not specified. 'yang' shall be the only value supported if specified.

The **configure system management-interface schema-path** CLI command can be used to configure the "schema-path" (default = "cf3:/YANG"). See the **schema-path** command description in [Classic and Model-Driven Management Interfaces Command Reference](#) for more information.

Operators should initially copy all the YANG files to the specified schema-path location.

A <get-schema> operation can not be used with the ALU base-r13 YANG set.

When the requested schema does not exist, the <error-tag> returned is "invalid-value".

When more than one schema matches the requested parameters, the <error-tag> returned is "operation-failed".

The following is an example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-schema xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
    <identifier>nokia-conf</identifier>
  </get-schema>
</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:ietf:params:xml:ns:yang:ietf-netconf-monitoring"><![CDATA[module nokia-conf {
    yang-version "1.1";
    namespace "urn:nokia.com:sros:ns:yang:sr:conf";
    ..
    ..
  }
]]></data>
```

</rpc-reply>

## 5.8 YANG Library

SR OS supports a mechanism, a YANG library, to identify the YANG modules and submodules that are implemented by the NETCONF server. NETCONF clients should be able to query or cache the YANG library contents and identify whether their cache is out-of-date.

The SR OS NETCONF server advertises the following capability in the <hello> message:

```
<capability>urn:ietf:params:netconf:capability:yang-library:1.0?revision=2018-05-08&module-set-id=<string></capability>
```

The following is the YANG Tree Diagram for the **modules-state**:

```
+--ro modules-state
  +--ro module-set-id    string
  +--ro module* [name revision]
    +--ro name            yang:yang-identifier
    +--ro revision        union
    +--ro schema?         inet:uri
    +--ro namespace       inet:uri
    +--ro feature*        yang:yang-identifier
    +--ro deviation* [name revision]
      | +--ro name        yang:yang-identifier
      | +--ro revision    union
    +--ro conformance-type enumeration
    +--ro submodule* [name revision]
      +--ro name          yang:yang-identifier
      +--ro revision      union
      +--ro schema?       inet:uri
```

The **module-set-id** is a mandatory leaf that identifies a set of YANG modules that the SR OS NETCONF server supports. The value of this leaf changes whenever there is a change in the set of modules or submodules in the YANG library. When this change occurs, SR OS changes the **module-set-id** value advertised in the NETCONF server <hello> message.

The **modules-state** can be used by the NETCONF client to fetch the YANG library, cache it and re-fetch it only if the value of the **module-set-id** changes again. The YANG library is returned in the **module** list.

Example:

1. If the SR OS NETCONF server advertises the following capability:

```
<capability>urn:ietf:params:netconf:capability:yang-library:1.0?revision=2018-05-08&module-set-id=1234</capability>
```

## 2. The NETCONF client can use the advertised **module-set-id** to query the YANG library:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="23">
  <get>
    <filter type="subtree">
      <modules-state xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-library">
        <module-set-id>1234</module-set-id>
        <module>
        </module>
      </modules-state>
    </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>
    <modules-state xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-library">
      <module-set-id>1234</module-set-id>
      <module>
        <name>iana-if-type</name>
        <revision>2014-05-08</revision>
        <schema></schema>
        <namespace>urn:ietf:params:xml:ns:yang:iana-if-type</namespace>
        <feature></feature>
        <conformance-type>implement</conformance-type>
      </module>
      ...
      ...
      <module>
        <name>nokia-conf</name>
        <revision>2016-07-06</revision>
        <schema></schema>
        <namespace>urn:nokia.com:sros:ns:yang:sr:conf</namespace>
        <feature></feature>
        <conformance-type>implement</conformance-type>
        <submodule>
          <name>nokia-conf-aa-common</name>
          <revision>2018-04-23</revision>
          <schema></schema>
        </submodule>
        ...
        ...
      </module>
      ...
      ...
    </modules-state>
  </data>
</rpc-reply>
]]>]]>
```



## 5.9 NETCONF Configuration Command Reference

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

- [Command Hierarchies](#)
- [Configuration Commands](#)

### 5.9.1 Command Hierarchies

#### 5.9.1.1 NETCONF System Commands

```
config
  — system
    — netconf
      — [no] auto-config-save
      — capabilities
        — [no] candidate
        — [no] writable-running
      — [no] shutdown
```

#### 5.9.1.2 NETCONF Security Commands

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

### 5.9.2 Configuration Commands

- [NETCONF System Commands](#)
- [NETCONF Security Commands](#)

---

### 5.9.2.1 NETCONF System Commands

#### auto-config-save

<b>Syntax</b>	<b>[no] auto-config-save</b>
<b>Context</b>	config>system>netconf
<b>Description</b>	This command is used to control whether committed changes are automatically persistent (that is, copied to the <startup> datastore) or not, when a commit is successful.
<b>Default</b>	no auto-config-save

#### candidate

<b>Syntax</b>	<b>[no] candidate</b>
<b>Context</b>	config>system>netconf>capabilities
<b>Description</b>	<p>This command enables or disables support of the candidate datastore in the SR OS NETCONF server. If the candidate is disabled then requests that reference the candidate datastore return an error, and when a NETCONF client establishes a new session the candidate capability is not advertised in the SR OS &lt;hello&gt;. This command also controls support of the &lt;commit&gt; and &lt;discard-changes&gt; operations.</p> <p>When <b>management-interface configuration-mode</b> is set to <b>classic</b>, then the candidate capability is disabled, even if <b>candidate</b> is configured.</p>
<b>Default</b>	candidate

#### writable-running

<b>Syntax</b>	<b>[no] writable-running</b>
<b>Context</b>	config>system>netconf>capabilities
<b>Description</b>	<p>This command enables or disables support of the writable-running capability in the SR OS NETCONF server. If writable-running is disabled then requests that reference the running datastore as a target return an error, and when a NETCONF client establishes a new session the writable-running capability is not advertised in the SR OS &lt;hello&gt;.</p> <p>When <b>management-interface configuration-mode</b> is set to <b>model-driven</b>, then the writable-running capability is disabled, even if <b>writable-running</b> is configured.</p>
<b>Default</b>	writable-running

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>netconf
<b>Description</b>	This command disables the NETCONF server. The <b>shutdown</b> command is blocked if there are any active NETCONF sessions. Use the <b>admin disconnect</b> command to disconnect all NETCONF sessions before shutting down the NETCONF service.

### 5.9.2.2 NETCONF Security Commands

## netconf

<b>Syntax</b>	<b>netconf</b>
<b>Context</b>	config>system>security>profile
<b>Description</b>	This command authorizes various netconf capabilities for the user.

## base-op-authorization

<b>Syntax</b>	<b>base-op-authorization</b>
<b>Context</b>	config>system>security>profile>netconf
<b>Description</b>	This command enables the context where permission to use various NETCONF operations is controlled.

## 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>	no kill-session

## lock

<b>Syntax</b>	[no] lock
<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 lock NETCONF operation. This lock operation allows a NETCONF client to lock the running datastore or the candidate datastore.
<b>Default</b>	no lock

---

## 5.10 NETCONF Show and Debug Command Reference

### 5.10.1 Command Hierarchies

#### 5.10.1.1 Show Commands

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

#### 5.10.1.2 Debug Commands

```
debug
  — system
    — netconf
      — info
```

### 5.10.2 Command Descriptions

#### 5.10.2.1 Show Commands

Command outputs shown in this section are examples only; actual displays may differ depending on supported functionality and user configuration.

##### 5.10.2.1.1 System Commands

netconf

<b>Syntax</b>	netconf
<b>Context</b>	show>system

**Description** This command displays NETCONF SSH sessions.

**Output** The following displays NETCONF information.

Table 78 describes the NETCONF output fields.

### Sample Output

```
# show system netconf
=====
NETCONF Server
=====
Administrative State      : Enabled
Operational State        : Up
-----
Connection      Username      Session Status      Running      Candidate
                  Id              Locked?             Locked?
-----
10.224.26.145    admin        17      connected      no          no
10.224.26.145    admin        15      connected      no          no
-----
Number of NETCONF sessions : 2
=====
```

**Table 78** Show System NETCONF Output Fields

Label	Description
Administrative State	Enabled — Displays that NETCONF is enabled. Disabled — Displays that NETCONF is disabled.
Operational State	Up — Displays that NETCONF is operational. Down — Displays that NETCONF is not operational.
Connection	The IP address of the connected router(s) (remote client).
Username	The name of the user.
Session ID	The NETCONF session ID.
Status	Connected or not connected.
Number of NETCONF sessions	Total NETCONF sessions
Running Locked?	Yes — Displays that the <running> datastore is locked. No — Displays that the <running> datastore is not locked.
Candidate Locked?	Yes — Displays that the <candidate> datastore is locked. No — Displays that the <candidate> datastore is not locked.

## counters

<b>Syntax</b>	<b>counters</b>
<b>Context</b>	show>system>netconf
<b>Description</b>	This command displays NETCONF counters.
<b>Output</b>	The following displays NETCONF counter information. <a href="#">Table 79</a> describes the NETCONF counter output fields.

### Sample Output

```
# show system netconf counters
=====
NETCONF counters:
=====
    Rx Messages
-----
    in gets           : 23
    in get-configs    : 19
    in edit-configs   : 35
    in copy-configs   : 0
    in delete-configs : 0
    in validates      : 0
    in close-sessions : 0
    in kill-sessions  : 0
    in locks          : 0
    in unlocks        : 0
    in commits        : 2
    in discards       : 1
-----
    Rx Total          : 80
=====
    Tx Messages
-----
    out rpc-errors    : 4
-----
    Tx Total          : 9
=====
    Failed requests due to lock being taken by other sessions
-----
    failed edit-configs: 1
    failed locks       : 0
=====
```

**Table 79** NETCONF Counters Output Fields

Label	Description
RX Messages	Types and numbers of received messages
RX Total	Total of all received messages

**Table 79**      **NETCONF Counters Output Fields (Continued)**

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

### 5.10.3 Debug Commands

Command outputs shown in this section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### 5.10.3.1 NETCONF Debug Commands

##### netconf

<b>Syntax</b>	<b>netconf</b>
<b>Context</b>	debug>system
<b>Description</b>	This command enters the debug NETCONF context.

##### info

<b>Syntax</b>	<b>info</b>
<b>Context</b>	debug>system>netconf
<b>Description</b>	This command displays debug information for NETCONF sessions.
<b>Output</b>	The following displays debug information for NETCONF sessions.

##### Sample Output

```
17 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
```



session started"

"18 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF  
NETCONF: INFO user: ncuser session 36:  
received <hello>"

19 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36: setting 1.1 capability, chunk framing mode e  
nabled"

20 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36:  
successfully processed <hello> message"

21 2018/03/17 12:29:54.844 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36:  
received <edit-config>"

22 2018/03/17 12:29:54.848 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36:  
error occurred while processing <edit-config> RPC"

23 2018/03/17 12:29:54.892 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36:  
successfully processed <edit-config> RPC"

24 2018/03/17 12:29:54.893 UTC minor: DEBUG #2001 Base NETCONF  
"NETCONF: INFO user: ncuser session 36:  
session terminated"



# 5.11 NETCONF Admin Command Reference

## 5.11.1 Command Hierarchies

### 5.11.1.1 Admin Commands



## 5.11.2 Command Descriptions

### 5.11.2.1 Admin Commands

Command outputs shown in this section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### discard-changes

<b>Syntax</b>	<b>discard-changes</b> <i>datastore-type</i>
<b>Context</b>	admin>system>candidate
<b>Description</b>	This operation discards uncommitted changes on the <candidate> datastore.
<b>Parameters</b>	<i>datastore-type</i> — Specifies the datastore type.
<b>Values</b>	global



## 6 Event and Accounting Logs

### 6.1 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 four 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.

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.
- A router name (also called a vrtr-name) identifying the associated routing context (for example, Base or vprn1000).
- A subject identifying the affected object for the event (e.g. interface name or port identifier).
- 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 80](#).

**Table 80** Event Severity Levels

Severity Number	Severity Name
1	cleared
2	indeterminate (info)

**Table 80 Event Severity Levels (Continued)**

Severity Number	Severity Name
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, router name (vrtr-name), 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 supported destination for an accounting log is a compact flash system device. Accounting data is stored within a standard directory structure on the device in compressed XML format. It is recommended that accounting logs be configured on the cf1: or cf2: devices only. Accounting log files are not recommended on the cf3: device (cf3: is intended to be used primarily for software images and configuration related files).

---

## 6.2 Log Destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. Routers support the following log destinations:

- [Console](#)
- [Session](#)
- [CLI Logs](#)
- [Memory Logs](#)
- [Log Files](#)
- [SNMP Trap Group](#)
- [Syslog](#)
- [NETCONF](#)

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.

### 6.2.1 Console

Sending events to a console destination means the message will be sent to the system console. The console device can be used as an event log destination.

### 6.2.2 Session

A session destination is a temporary log destination which directs entries to the active telnet or SSH session for the duration of the session. When the session is terminated, for example, when the user logs out, the “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.

---

## 6.2.3 CLI Logs

A CLI log is a log that outputs log events to a CLI session. An operator can subscribe to a CLI log from within a CLI session using the **tools perform log subscribe-to log-id** command. The events are sent to the CLI session for the duration of that CLI session (or until an **unsubscribe-from** command is issued).

## 6.2.4 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.

## 6.2.5 Log Files

Log files can be used by both event logs and accounting logs and are stored on the compact flash devices in the file system. It is recommended that event and accounting logs be configured on the cf1: or cf2: devices only. Log files are not recommended on the cf3: device (cf3: is intended to be used primarily for software images and configuration related files).

A log file is identified with a single log file ID, but a log file will generally be composed of a number individual files in the file system. A log file is configured with a rollover parameter, expressed in minutes, which represents the length of time an individual log file should be written to before a new file is created for the relevant log file ID. The rollover time is checked only when an update to the log is performed. Thus, complying to this rule is subject to the incoming rate of the data being logged. For example, if the rate is very low, the actual rollover time may be longer than the configured value.

The retention time for a log file specifies the amount of time the file should be retained on the system based on the creation date and time of the file.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file.

Event log files are always created in the **\log** directory on the specified compact flash device. The naming convention for event log files is:



*log eeff-timestamp*

where:

*ee* is the event log ID

*ff* is the log file destination ID

*timestamp* is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

*yyyy* is the four-digit year (for example, 2007)

*mm* is the two digit number representing the month (for example, 12 for December)

*dd* is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

*hh* is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

*mm* is the two digit minute (for example, 30 for 30 minutes past the hour)

*ss* is the two digit second (for example, 14 for 14)

Accounting log files are created in the **act-collect** directory on a compact flash device (specifically *cf1* or *cf2*). The naming convention for accounting log files is nearly the same as for log files except the prefix **act** is used instead of the prefix **log**. The naming convention for accounting logs is:

*act aaff-timestamp.xml.gz*

where:

*aa* is the accounting policy ID

*ff* is the log file destination ID

*timestamp* is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

*yyyy* is the four-digit year (for example, 2007)

*mm* is the two digit number representing the month (for example, 12 for December)

*dd* is the two digit number representing the day of the month (for example, 03 for the 3rd of the month)

*hh* is the two digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

*mm* is the two digit minute (for example, 30 for 30 minutes past the hour)

*ss* is the two digit second (for example, 14 for 14 seconds)

Accounting logs are .xml files created in a compressed format and have a .gz extension.

The **\act-collect** directory is where active accounting logs are written. When an accounting log is rolled over, the active file is closed and archived in the **\act** directory before a new active accounting log file created in **\act-collect**.

When creating a new log file on a Compact Flash disk card, the system will check the amount of free disk space and that amount must be greater than or equal to the lesser of 5.2 MB or 10% of the Compact Flash disk capacity.

## 6.2.6 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.

## 6.2.7 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 to 23) (default 23 - local 7).
- The Syslog Severity Threshold (0 to 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 81](#) displays the severity level mappings to syslog severities.

**Table 81 Router to Syslog Severity Level Mappings**

SR OS Event Severity	Syslog Severity Numerical Code	Syslog Severity Name	Syslog Severity Definition
--	0	emergency	System is unusable
critical (3)	1	alert	Action must be taken immediately
major (4)	2	critical	Critical conditions
minor (5)	3	error	Error conditions
warning (6)	4	warning	Warning conditions
--	5	notice	Normal but significant condition
cleared (1) indeterminate (2)	6	info	Informational messages
--	7	debug	Debug-level messages

The general format of an SR OS syslog message is as follows (see RFC 3164, *The BSD Syslog Protocol*). The “<” and “>” are informational delimiters to make reading and understanding the format easier and they do not appear in the actual syslog message except as part of the PRI:

<PRI> <HEADER><MSG>

where:

- **<PRI/>** (the "<" and ">" are included in the syslog message) is the configured facility\*8+severity (as described in the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR System Management Guide* and RFC3164).
- **<HEADER>** is "MMM DD HH:MM:SS <source IP addr>" (without the quotes). There are always 2 characters for the day (DD). Single digit days are preceded with a space character.
- **<MSG>** is <log-prefix>: <seq> <vrtr-name> <application>-<severity>-<Event Name>-<Event ID> [<subject>]: <message>\n

where:

- **<log-prefix>** is an optional 32 characters of text (default = 'TMNX') as configured in the log-prefix command.
- **<seq>** is the log event sequence number (always preceded by a colon and a space char)
- **<vrtr-name>** is vprn1, vprn2, ... | Base | management | vpls-management
- **<subject>** may be empty resulting in []:
- \n is the standard ASCII new line character (hex 0A)

Examples (from different nodes):

#### default log-prefix (TMNX):

```
<188>Jan  2 18:43:23 10.221.38.108 TMNX: 17 Base SYSTEM-WARNING-tmnxStateChange-
2009 [CHASSIS]:  Status of Card 1 changed administrative state: inService,
operational state: outOfService\n
<186>Jan  2 18:43:23 10.221.38.108 TMNX: 18 Base CHASSIS-MAJOR-tmnxEqCardRemoved-
2003 [Card 1]:  Class IO Module : removed\n
```

#### no log-prefix:

```
<188>Jan 11 18:48:12 10.221.38.108 : 32 Base SYSTEM-WARNING-tmnxStateChange-2009
[CHASSIS]:  Status of Card 1 changed administrative state: inService,
operational state: outOfService\n
<186>Jan 11 18:48:12 10.221.38.108 : 33 Base CHASSIS-MAJOR-tmnxEqCardRemoved-
2003 [Card 1]:  Class IO Module : removed\n
```

#### log-prefix "test":

```
<186>Jan 11 18:51:22 10.221.38.108 test: 47 Base CHASSIS-MAJOR-tmnxEqCardRemoved-
2003 [Card 1]:  Class IO Module : removed\n
<188>Jan 11 18:51:22 10.221.38.108 test: 48 Base SYSTEM-WARNING-tmnxStateChange-
2009 [CHASSIS]:  Status of Card 1 changed administrative state: inService,
operational state: outOfService\n
```

## 6.2.8 NETCONF

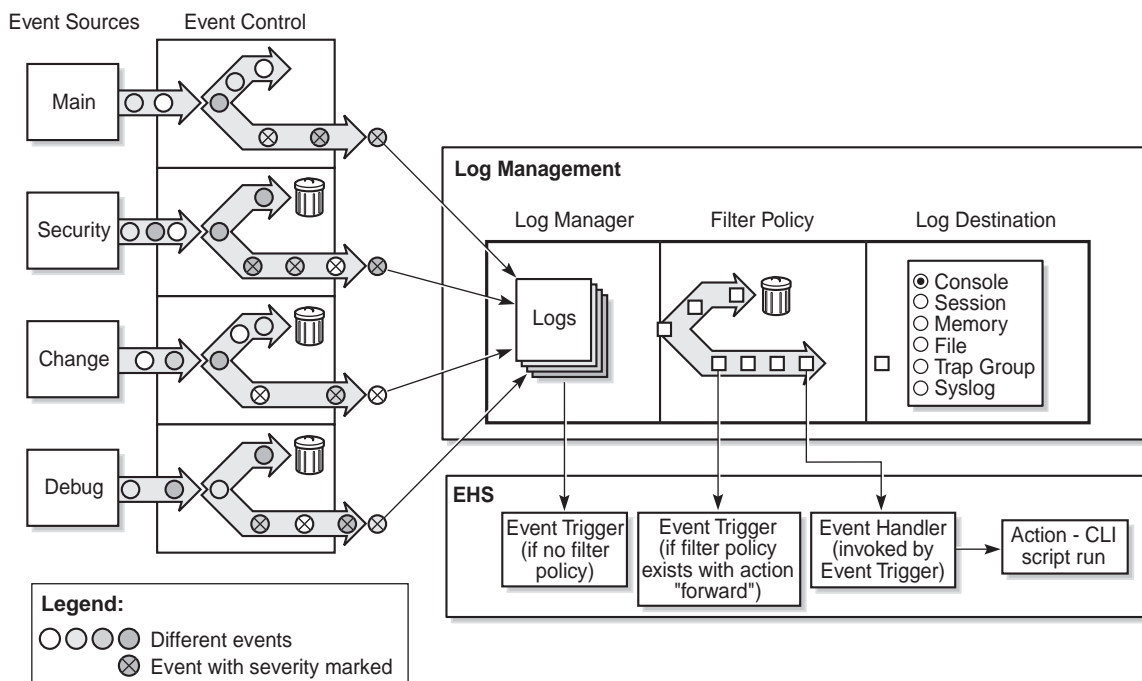
A NETCONF log is a log that outputs log events to a NETCONF session as notifications. A NETCONF client can subscribe to a NETCONF log using the configured **netconf-stream** *stream-name* for the log in a subscription request. See [NETCONF Notifications](#) for more details.

## 6.3 Event Logs

Event logs are the means of recording system generated events for later analysis. Events are messages generated by the system by applications or processes within the router.

Figure 17 depicts a function block diagram of event logging.

**Figure 17 Event Logging Block Diagram**



27853

### 6.3.1 Event Sources

In Figure 17, 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, and so on. 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
...
USER
VRRP
VRTR
=====
*A:ALA-48#
```

## 6.3.2 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](#).

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
-----
show
BGP:
  2001 bgpEstablished                          MI  gen     1         0
  2002 bgpBackwardTransition                   WA  gen     7         0
  2003 tBgpMaxPrefix90                         WA  gen     0         0
...
CCAG:
CFLOWD:
  2001 cflowdCreated                          MI  gen     1         0
  2002 cflowdCreateFailure                     MA  gen     0         0
  2003 cflowdDeleted                          MI  gen     0         0
...
CHASSIS:
  2001 cardFailure                            MA  gen     0         0
  2002 cardInserted                           MI  gen     4         0
  2003 cardRemoved                            MI  gen     0         0
...
'''
DEBUG:
L 2001 traceEvent                             MI  gen     0         0
DOT1X:
FILTER:
  2001 filterPBRPacketsDropped                 MI  gen     0         0
```



---

```
IGMP:
  2001 vRtrIgmpIfRxQueryVerMismatch    WA  gen      0      0
  2002 vRtrIgmpIfCModeRxQueryMismatch  WA  gen      0      0
IGMP_SNOOPING:
IP:
L  2001 clearRTMError                  MI  gen      0      0
L  2002 ipEtherBroadcast                MI  gen      0      0
L  2003 ipDuplicateAddress              MI  gen      0      0
...
ISIS:
  2001 vRtrIsisDatabaseOverload         WA  gen      0      0
```

### 6.3.3 Log Manager and Event Logs

Events that are forwarded by event control are sent to the log manager. The log manager manages the event logs in the system and the relationships between the log sources, event logs and log destinations, and log filter policies.

An event log has the following properties:

- A unique log ID — The log ID is a short, numeric identifier for the event log. A maximum of 15 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 (for example, syslog or memory).
- An optional event filter policy — An event filter policy defines whether to forward or drop an event or trap-based on match criteria.

### 6.3.4 Event Filter Policies

The log manager uses event filter policies to allow fine control over which events are forwarded or dropped based on various criteria. Like other filter policies in the SR OS, 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 82](#):

**Table 82** 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.

### 6.3.5 Event Log Entries

Log entries that are forwarded to a destination are formatted in a way appropriate for the specific destination whether it be recorded to a file or sent as an SNMP trap, but log event entries have common elements or properties. All application generated events have the following properties:

- A time stamp in UTC or local time.
- The generating application.

- A unique event ID within the application.
- A router name (vrtr-name, for example, vprn101 or Base) identifying the router instance 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 <time> TZONE <severity>: <application> #<event_id> <vrtr-name>
<subject>
<message>
```

The following is an event log example:

```
252 2013/05/07 16:21:00.761 UTC WARNING: SNMP #2005 Base my-interface-abc
"Interface my-interface-abc is operational"
```

The specific elements that compose the general format are described in [Table 83](#).

**Table 83** Log Entry Field Descriptions

Label	Description
nnnn	The log entry sequence number.
<time>	YYYY/MM/DD HH:MM:SS.SSS
YYYY/MM/DD	The UTC date stamp for the log entry. YYYY — Year MM — Month DD — Date
HH:MM:SS.SSS	The UTC time stamp for the event. HH — Hours (24 hour format) MM — Minutes SS.SSS — Seconds
TZONE	The timezone (for example, UTC, EDT) as configured by <b>configure log log-id x time-format</b> .

**Table 83** Log Entry Field Descriptions (Continued)

Label	Description
<severity>	The severity level name of the event. CLEARED — A cleared event (severity number 1). INFO — An indeterminate/informational severity event (severity level 2). CRITICAL — A critical severity event (severity level 3). MAJOR — A major severity event (severity level 4). MINOR — A minor severity event (severity level 5). WARNING — A warning severity event (severity 6).
<application>	The application generating the log message.
<event_id>	The application's event ID number for the event.
<vrtr-name>	The router name (vrtr-name, for example, vprn101 or Base) representing the router instance that generated the event.
<subject>	The subject/affected object for the event.
<message>	A text description of the event.

### 6.3.6 Simple Logger Event Throttling

Simple event throttling provides a mechanism to protect event receivers from being overloaded when a scenario causes many events to be generated in a very short period of time. A throttling rate, # events/# seconds, can be configured. Specific event types can be configured to be throttled. 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.

## 6.3.7 Default System Log

Log 99 is a pre-configured memory-based log which logs events from the main event source (not security, debug, and so on). 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#
```

## 6.3.8 Event Handling System

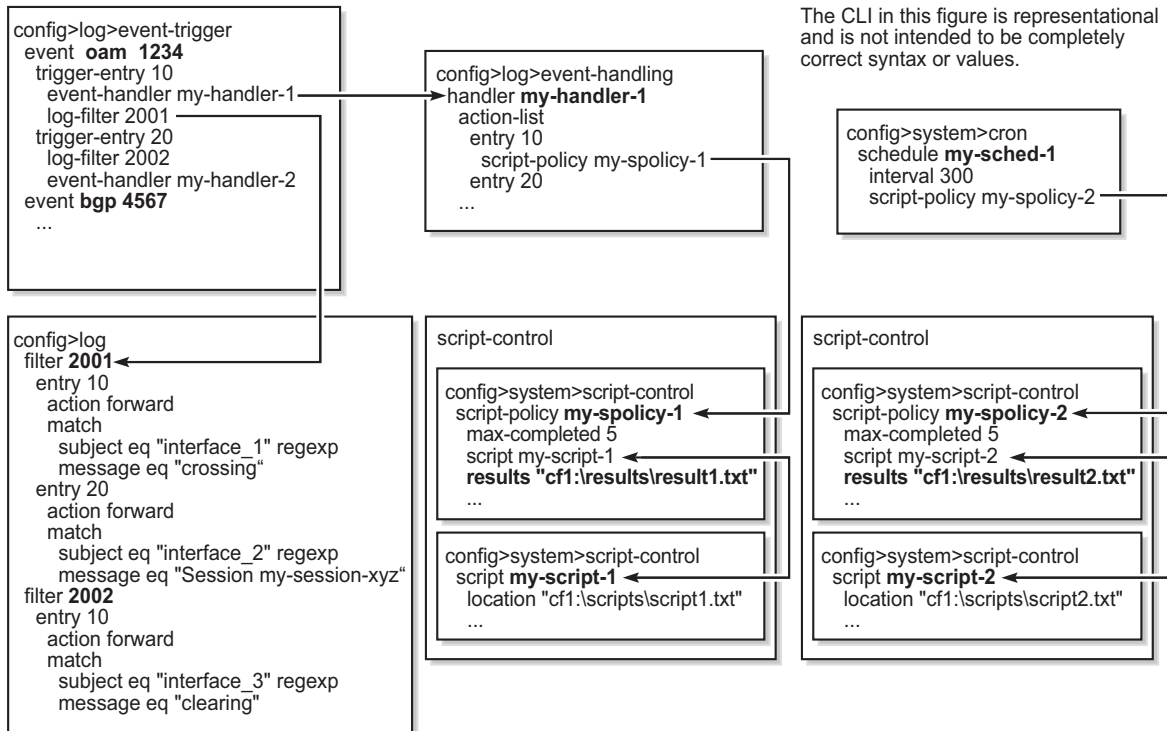
The Event Handling System (EHS) is a framework that allows operator-defined behavior to be configured on the router. EHS adds user-controlled programmatic exception handling by allowing a CLI script to be executed upon the detection of a log event (the 'trigger'). Regexp style expression matching is 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. [Figure 18](#) illustrates the relationships between the different configurable objects used by EHS (and CRON).

**Figure 18 EHS Object Relationships**



24884

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.

Varbinds are variable bindings that represent the variable number of values that are included in a log event.

A triggering log event's common parameters and varbinds are passed in to the triggered EHS script and can be used within the EHS script as passed-in (dynamic) variables. Passed-in (dynamic) variables are:

- the common event parameters, for example: appid, name, eventid, severity, subject, and gentime.
- the predefined varbinds in a log event's message.

For example, the following are the passed-in (dynamic) variables for an event:

- appid
- eventid
- severity
- subject
- gentime
- event\_varbind\_1
- event\_varbind\_2
- ...
- ...
- event\_varbind\_N



**Note:**

- For more information about showing event parameters, see the show commands in [Log Configuration Command Reference](#).
- Refer to the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR Log Events Guide* for any event's predefined varbinds
- The passed-in event's **gentime** is always UTC
- The event's sequence number is not passed in to the script

When using the classic CLI, an EHS script has the ability to define local (static) variables and use some basic `.if/.set` commands inside the script. The use of variables with `.if/.set` commands within an EHS script adds more logic to the EHS scripting and allows the reuse of a single EHS script for more than one trigger or action.

Both passed-in and local variables can be used within the EHS script either as part of the CLI commands or as part of the `.if/.set` commands.

The following applies to both CLI commands and `.if/.set` commands (where X represents a variable).

- Using `$X`, without using single or double quotes, replaces the variable `X` with its string or integer value.
- Using `"X"`, with double quotes, means the literal string `X`.
- Using `"$X"`, with double quotes, replaces the variable `X` with its string or integer value.
- Using `'X'`, with single quotes, means the literal string `X`.
- Using `'$X'`, with single quotes, does not replace the variable `X` with its value but means the literal string `$X`.

In summary:

- All characters within single quotes are interpreted as a string character.
- All characters within double quotes are interpreted as regular characters except for `$`, which replaces the variable with its value (for example, shell expansion inside a string).

Some supported scenarios are (note that the following are pseudo commands):

- `.if $string_variable==string_value_or_string_variable {`  
    `CLI_commands_set1`  
    `.} else {`  
        `CLI_commands_set2`  
    `.} endif`
- `.if ($string_variable==string_value_or_string_variable) {`  
    `CLI_commands_set1`  
    `.} else {`  
        `CLI_commands_set2`  
    `.} endif`
- `.if $integer_variable==integer_value_or_integer_variable {`  
    `CLI_commands_set1`  
    `.} else {`  
        `CLI_commands_set2`  
    `.} endif`
- `.if ($integer_variable==integer_value_or_integer_variable) {`  
    `CLI_commands_set1`  
    `.} else {`  
        `CLI_commands_set2`  
    `.} endif`



- *.if \$string\_variable!=string\_value\_or\_string\_variable* {  
    *CLI\_commands\_set1*  
} else {  
    *CLI\_commands\_set2*  
} endif
- *.if (\$string\_variable!=string\_value\_or\_string\_variable)* {  
    *CLI\_commands\_set1*  
} else {  
    *CLI\_commands\_set2*  
} endif
- *.if \$integer\_variable!=integer\_value\_or\_integer\_variable* {  
    *CLI\_commands\_set1*  
} else {  
    *CLI\_commands\_set2*  
} endif
- *.if (\$integer\_variable!=integer\_value\_or\_integer\_variable)* {  
    *CLI\_commands\_set1*  
} else {  
    *CLI\_commands\_set2*  
} endif
- *.set \$string\_variable = string\_value\_or\_string\_variable*
- *.set (\$string\_variable = string\_value\_or\_string\_variable)*
- *.set \$integer\_variable = integer\_value\_or\_integer\_variable*
- *.set (\$integer\_variable = integer\_value\_or\_integer\_variable)*

where:

- *CLI\_commands\_set1* is a set of one or more CLI commands
- *CLI\_commands\_set2* is a set of one or more CLI commands
- *string\_variable* is a local (static) string variable
- *string\_value\_or\_string\_variable* is a string value/variable
- *integer\_variable* is a local (static) integer variable
- *integer\_value\_or\_integer\_variable* is an integer value/variable

**Note:**

- A limit of 100 local (static) variables per EHS script is imposed. Exceeding this limit may result in an error and partial execution of the script.
- When a set statement is used to set a string\_variable to a string\_value, the string\_value can be any non-integer value not surrounded by single/double quotes or it can be surrounded by single/double quotes
- A "." preceding a directive (for example, if, set...and so on) is always expected to start a new line
- An end of line is always expected after {
- A CLI command is always expected to start a new line
- Passed-in (dynamic) variables are always read only inside an EHS script and cannot be overwritten using a set statement
- .if commands support == and != operators only
- .if and .set commands support addition, subtraction, multiplication, and division of integers
- .if and .set commands support addition of strings which means "concatenation" of strings

**Valid Examples:**

- configure service epipe \$serviceID  
where *\$serviceID* is either a local (static) integer variable or passed-in (dynamic) integer variable
- echo srcAddr is \$srcAddr  
where *\$srcAddr* is a passed-in (dynamic) string variable
- .set \$ipAddr = "10.0.0.1"  
where *\$ipAddr* is a local (static) string variable
- .set \$ipAddr = \$srcAddr  
where *\$srcAddr* is a passed-in (dynamic) string variable  
*\$ipAddr* is a local (static) string variable.
- .set (\$customerID = 50)  
where *\$customerID* is a local (static) integer variable
- .set (\$totalPackets = \$numIngrPackets + \$numEgrPackets)  
where *\$totalPackets*, *\$numIngrPackets*, *\$numEgrPackets* are local (static) integer variables
- .set (\$portDescription = \$portName + \$portLocation)  
where *\$portDescription*, *\$portName*, *\$portLocation* are local (static) string variables

- if (\$srcAddr == "CONSOLE") {  
    *CLI\_commands\_set1*  
  } else {  
    *CLI\_commands\_set2*  
  } endif  
  where *\$srcAddr* is a passed-in (dynamic) string variable  
    *CLI\_commands\_set1* is a set of one or more CLI commands  
    *CLI\_commands\_set2* is a set of one or more CLI commands
- .if (\$customerID == 10) {  
    *CLI\_commands\_set1*  
  } else {  
    *CLI\_commands\_set2*  
  } endif  
  where *\$customerID* is a passed-in (dynamic) integer variable  
    *CLI\_commands\_set1* is a set of one or more CLI commands  
    *CLI\_commands\_set2* is a set of one or more CLI commands
- .if (\$numIngrPackets == \$numEgrPackets) {  
    *CLI\_commands\_set1*  
  } else {  
    *CLI\_commands\_set2*  
  } endif  
  where *\$numIngrPackets* and *\$numEgrPackets* are local (static) integer variables  
    *CLI\_commands\_set1* is a set of one or more CLI commands  
    *CLI\_commands\_set2* is a set of one or more CLI commands

**Invalid Examples:**

- .set \$srcAddr = "10.0.0.1"  
  where *\$srcAddr* is a passed-in (dynamic) string variable  
  Reason: passed-in variables are read only inside an EHS script.
- .set (\$ipAddr = \$numIngrPackets + \$numEgrPackets)  
  where *\$ipAddr* is a local (static) string variable  
    *\$numIngrPackets* and *\$numEgrPackets* are local (static) integer variables  
  Reason: variable types do not match, cannot assign a string to an integer.
- .set (\$numIngrPackets = \$ipAddr + \$numEgrPackets)

where *\$ipAddr* is a local (static) string variable

*\$numIngrPackets* and *\$numEgrPackets* are local (static) integer variables

Reason: variable types do not match, cannot concatenate a string to an integer.

- .set *\$ipAddr* = "10.0.0.1"100

where *\$ipAddr* is a local (static) string variable

Reason: when double quotes are used, they have to surround the entire string.

- .if (*\$totalPackets* == "10.1.1.1") {  
  .} endif

where *\$totalPackets* is a local (static) integer variables

Reason: cannot compare an integer variable to a string value.

- .if (*\$ipAddr* == 10) {  
  .} endif

where *\$ipAddr* is a local (static) string variable

Reason: cannot compare a string variable to an integer value.

- .if (*\$totalPackets* == *\$ipAddr*) {

where *\$totalPackets* is a local (static) integer variables

*\$ipAddr* is a local (static) string variable

Reason: cannot compare an integer variable to a string variable.

## EHS debounce

EHS debounce (also called dampening) is the ability to trigger an action (for example an EHS script), if an event happens (N) times within a specific time window (S).

N = [2..15]

S = [1..604800]



### Note:

- Triggering happens with the Nth event not at the end of S
- There is no sliding window (for example a trigger at Nth event, N+1 event, and so on), as N is reset after a trigger and count is restarted
- When EHS debouncing/dampening is used, the varbinds passed in to an EHS script at script triggering time are from the Nth event occurrence (the Nth triggering event)
- If S is not specified then the SR OS will continue to trigger every Nth event

For example:

When linkDown occurs N times in S sec, an EHS script is triggered to shut down the port.

### 6.3.8.1 Executing EHS/CRON Scripts

The execution of EHS/CRON scripts depends on the CLI engine associated with the configuration mode. The EHS/CRON script execution engine is based on the primary CLI engine set by the CLI command **configure system management-interface cli cli-engine**.

For example, if **cli-engine** is configured to **classic-cli md-cli**, the script executes in the classic CLI infrastructure and disregards the configuration mode, even if it is model-driven.

The following describes the default behavior of the EHS/CRON scripts, depending on the configuration mode.

- Classic CLI configuration mode  
EHS/CRON scripts execute in the classic CLI environment and an error occurs if any model-driven CLI commands exist.
- Model-driven configuration mode  
EHS/CRON scripts execute in the MD-CLI environment and an error occurs if any classic CLI commands exist.
- Mixed configuration mode  
EHS/CRON scripts execute in the classic CLI environment and an error occurs if any model-driven CLI commands exist.

EHS/CRON scripts that contain MD-CLI commands can be used in the MD-CLI as follows:

- scripts can be configured
- scripts can be created, edited, and results read through FTP
- scripts can be triggered and executed
- scripts generate an error if there are any non MD-CLI commands or any `.if/.set` syntax in the script

User authorization for EHS/CRON scripts can be configured in either the classic CLI or the MD-CLI as follows:

- classic CLI  
**configure>system>security>cli-script>authorization>event-handler>cli-user** *user-name*

- MD-CLI

**configure system security cli-script authorization event-handler cli-user**  
*user-name*

When a user is not specified, an EHS/CRON script bypasses authorization and can execute all commands.

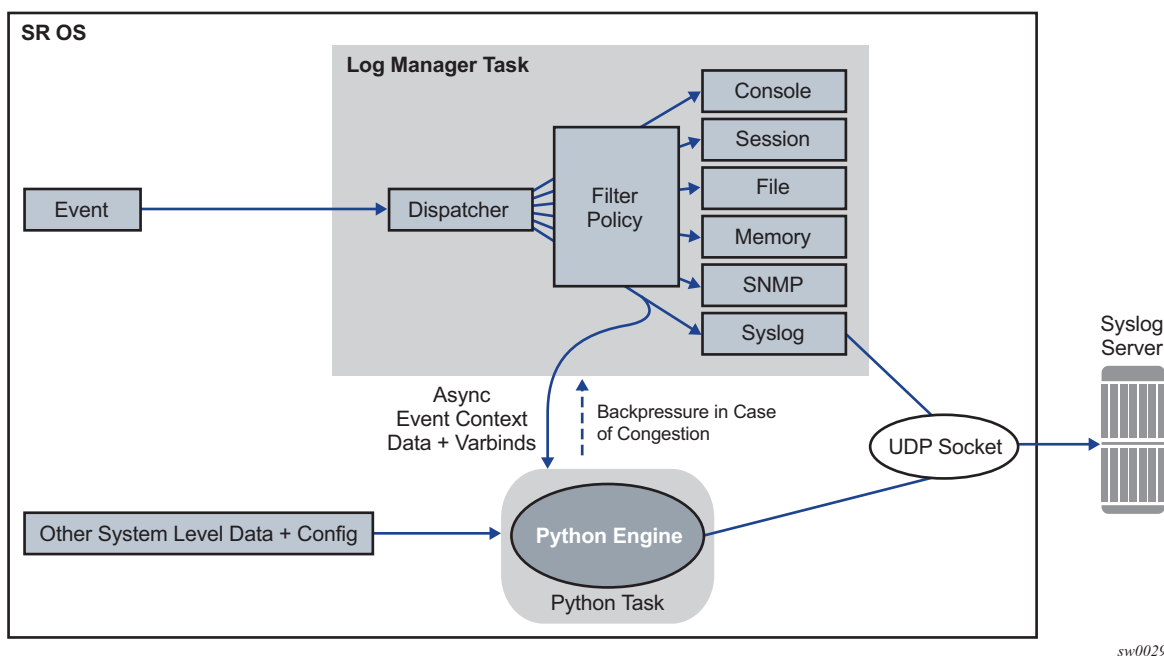
In all configuration modes, a script policy can be disabled (using the MD-CLI command **configure system script-control script-policy *policy-name* admin-state disable** or the classic-CLI command **configure>system>script-control>script-policy *policy-name*>shutdown**) even if history exists. When the script policy is disabled, the following applies.

- Newly triggered EHS/CRON scripts are not allowed to execute or queue.
- In-progress EHS/CRON scripts are allowed to continue.
- Already queued EHS/CRON scripts are allowed to execute.

## 6.4 Customizing Syslog Messages Using Python

Log events in SR OS can be customized by a Python script before they are sent to a syslog server. The log events that are subject to Python processing are selected via log filters. This allows only a preferred subset of log messages to be customized (Figure 19).

**Figure 19** Interaction between the Logger and the Python Engine



### 6.4.1 Python Engine for Syslog

This section discusses syslog-specific aspects of Python processing. Refer to the “Python Script Support for ESM” section of the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide* for an introduction to Python.

When an event is dispatched to the log manager in SR OS, the log manager asynchronously passes the event context data and varbinds to the Python engine, that is, the logger task is not waiting for feedback from Python. Varbinds are variable bindings that represent the variable number of values that are included in the event. Each varbind consists of a triplet (OID, type, value). Along with other system-level variables, the Python engine constructs a syslog message and sends it to the syslog destination. During this process, the operator can modify the format of the syslog message or leave it intact, as if it was generated by the syslog process within the log manager.

The tasks of the Python engine in a syslog context are as follows:

- assembles custom syslog messages (including PRI, HEADER and MSG fields) based on the received event context data, varbinds specific to the event, system-level data, and the configuration parameters (syslog server IP address, syslog facility, log-prefix and the destination UDP port)
- reformats timestamps in a syslog message
- sends the original or modified message to the syslog server
- drops the message

### 6.4.1.1 Python Syslog APIs

Python APIs are used to assemble a syslog message which, in SR OS, has the following generic format:

```
PRI> <HEADER><MSG>
```

where:

- **<PRI>** (the “<” and “>” are included in the syslog message) is the configured facility x 8+severity (as described in the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR System Management Guide* and RFC 3164)
- **<HEADER>** is MMM DD HH:MM:SS <hostname>. There are always two characters for the day (DD). Single digit days are preceded with a space character.
- **<MSG>** is <log-prefix>: <seq> <router-name> <application>-<severity>-<Event Name>-<Event ID> [<subject>]: <message>\n

where:

- **<log-prefix>** is an optional set of 32 characters (default = 'TMNX') as configured in the **log-prefix** command



- `<seq>` is the log event sequence number. It always preceded by a colon and a space character.
- `<router-name>` is the name of the router, for example, vprn1, vprn2, Base, management, vpls-management
- `<subject>` is the topic and can be empty, resulting in []:
- `\n` is the standard ASCII new line character (hex 0A)

Table 84 describes Python information that can be used to manipulate syslog messages.

**Table 84** Manipulating Python Syslog Messages

Imported Nokia (ALC) Modules	Access Rights	Comments
event (from alc import event)	—	The method used to retrieve generic event information.
syslog (from alc import syslog)	—	The method used to retrieve syslog-specific parameters.
system (from alc import system)	—	The method used to retrieve system-specific information. Currently, the only parameter retrieved is the system name.
Events use the following format as they are written into memory, file, console, and system: nnnn <time> <severity>:<application> # <event_id> <router-name> <subject> <message> The event-related information received in the context data from the log manager is retrieved via the following Python methods:		
event.sequence	RO	The sequence number of the event (nnnn).
event.timestamp	RO	The timestamp of the event. (YYYY/MM/DD HH:MM:SS.SS).
event.routerName	RO	The router name, for example, BASE, VPRN1, and so on.
event.application	RO	The application generating the event, for example, NA.
event.severity	RO	The severity of the event. This is configurable in SR OS (CLEARED [1], INFO [2], CRITICAL [3], MAJOR [4], MINOR [5], WARNING [6]).
event.eventId	RO	The event ID, for example, 2012.
event.eventName	RO	The event Name, for example, tmnxNatPIBoclAllocationLsn.
event.subject	RO	An optional field, for example, [NAT].

**Table 84** Manipulating Python Syslog Messages (Continued)

Imported Nokia (ALC) Modules	Access Rights	Comments
event.message	RO	The event-specific message, for example, "{2} Map 192.168.20.29 [2001-2005] MDA 1/2 -- 276824064 classic-lsn-sub %3 vpn1 10.10.10.101 at 2015/08/31 09:20:15".
Syslog Methods		
syslog.hostName	RO	The IP address of the SR OS node sending the syslog message. This is used in the Syslog HEADER.
syslog.logPrefix	RO	The log prefix which is configurable and optional, for example, TMNX:
syslog.severityToPRI(event.severity)	—	The Python method used to derive the PRI field in syslog header based on event severity and a configurable syslog facility.
syslog.severityToName(event.severity)	—	An SR OS event severity to syslog severity name. For more information, see the <a href="#">6.2.7</a> section.
syslog.timestampToUnix(timestamp)		The Python method that takes a timestamp in the format if YYYY/MM/DD HH:MM:SS and converts it into a UNIX-based format (seconds since Jan 01 1970 – UTC).
syslog.set(newSyslogPdu)	—	The Python method used to send the syslog message in the newSyslogPdu. This variable must be constructed manually via string manipulation. In the absence of the command, the SR OS assembles the default syslog message (as if Python was not configured) and sends it to the syslog server, assuming that the message is not explicitly dropped.
syslog.drop()	—	The Python method used to drop a syslog message. This method must be called before the syslog.set<newSyslogPdu> method.
System Methods		
system.name	RO	The Python method used to retrieve the system name

For example, assume that the syslog format is:

```
<PRI><timestamp> <hostname> <log-prefix>: <sequence> <router-name> <appid>-
```

```
<severity>-<name>-<eventid> [<subject>]: <text>
```

Then the following is an example of the syslogPdu constructed via Python:

```
syslogPdu = "<" + syslog.severityToPRI(event.severity) + ">" \
    + event.timestamp + " \
    " \ + syslog.hostname + " " + syslog.logPrefix + ": " + \
    event.sequence + " " + event.routerName + " " + \
    event.application + "- \
    " + \ syslog.severityToName(event.severity) + "- " + \
    event.eventName + "- " + event.eventId + " [" + \
    event.subject + "]: " + event.message
```

### 6.4.1.2 Timestamp Format Manipulation

Certain logging environments require customized formatting of the timestamp. Nokia provides a timestamp conversion method in the alu.syslog Python module to convert a timestamp from the format YYYY/MM/DD hh:mm:ss into a UNIX-based timestamp format (seconds since Jan 01 1970 – UTC).

For example, an operator can use the following Python method to convert a timestamp from the YYYY/MM/DD hh:mm:ss.ss or YYYY/MM/DD hh:mm:ss (no centiseconds) format into either the UNIX timestamp format or the MMM DD hh:mm:ss format.

```
from alu import event
from alu import syslog
from alu import system
#input format: YYYY/MM/DD hh:mm:ss.ss or YYYY/MM/DD hh:mm:ss
#output format 1: MMM DD hh:mm:ss
#output format 2: unixTimestamp (TBD)
def timeFormatConversion(timestamp,format):
    if format not in range(1,2):
        raise NameError('Unexpected format, expected:' \
            '0<format<3 got: '+str(format))
    try:
        dat,tim=timestamp.split(' ')
    except:
        raise NameError('Unexpected timestamp format, expected:' \
            'YYYY/MM/DD hh:mm:ss got: '+timestamp)
    try:
        YYYY,MM,DD=dat.split('/')
    except:
        raise NameError('Unexpected timestamp format, expected:' \
            'YYYY/MM/DD hh:mm:ss got: '+timestamp)
    try:
        hh,mm,ss=tim.split(':')
        ss=ss.split('.')[0] #just in case that the time format is hh:mm:ss.ss
    except:
        raise NameError('Unexpected timestamp format, expected:' \
            'YYYY/MM/DD hh:mm:ss got: '+timestamp)
    if not (1970<=int(YYYY)<2100 and
        1<=int(MM)<=12 and
        1<=int(DD)<=31 and
```

---

```

        0<=int(hh)<=24 and
        0<=int(mm)<=60 and
        0<=int(ss)<=60):
            raise NameError('Unexpected timestamp format, or values out of the range' \
                             'Expected: YYYY/MM/DD hh:mm:ss got: '+timestamp)
    if format == 1:
        MMM={1:'Jan',
              2:'Feb',
              3:'Mar',
              4:'Apr',
              5:'May',
              6:'Jun',
              7:'Jul',
              8:'Aug',
              9:'Sep',
              10:'Oct',
              11:'Nov',
              12:'Dec'}[int(MM)]
        timestamp=MMM+' '+DD+' '+hh+':'+mm+':'+ss
    if format == 2:
        timestamp=syslog.timestampToUnix(timestamp)
    return timestamp

```

The `timeFormatConversion` method can accept the `event.timestamp` value in the format:

```
YYYY/MM/DD HH:MM:SS.SS
```

and return a new timestamp in the format determined by the `format` parameter:

```

1 ? MMM DD HH:MM:SS
2 ? Unix based time format

```

This method accepts the input format in either of the two forms `YYYY/MM/DD HH:MM:SS.SS` or `YYYY/MM/DD HH:MM:SS` and simply ignores the centisecond part in the former form.

## 6.4.2 Python Processing Efficiency

Python retrieves event-related variables from the log manager, as opposed to retrieving pre-assembled syslog messages. This eliminates the need for string parsing of the syslog message to manipulate its constituent parts, increasing the speed of Python processing.

To further improve processing performance, Nokia recommends performing string manipulation via the Python native string method, when possible.

## 6.4.3 Python Backpressure

A Python task assembles syslog messages based on the context information received from the logger and sends them to the syslog server independent of the logger. If the Python task is congested due to a high volume of received data, the backpressure should be sent to the ISA so that the ISA stops allocating NAT resources. This behavior matches the current behavior in which NAT resources allocation is blocked if that logger is congested.

## 6.4.4 Event Selection for Python Processing

Events destined for Python processing are configured through a log ID that references a Python policy. The selection of the events are performed via a filter associated with this log ID. The remainder of the events destined to the same syslog server can bypass Python processing by redirecting them to a different log ID. The following example clarifies this point:

### 1. Creating the Python policy

```
A:dut-a# configure python python-policy PyForLogEvents create
*A:dut-a>config>python>py-policy$
[no] description      - Configure the description of this policy
[no] dhcp             - Configure scripts to handle dhcp messages jitter
[no] dhcp6            - Configure scripts to handle dhcp6 messages
[no] diameter         - Configure scripts to handle diameter messages
[no] gtpv1-c          - Configure scripts to handle GTPv1-C messages
[no] gtpv2-c          - Configure scripts to handle GTPv2-C messages
[no] pppoe            - Configure scripts to handle PPPoE messages
[no] radius           - Configure scripts to handle RADIUS messages
[no] vsd              - Configure scripts to handle VSD messages
[no] syslog           - Configure a script to handle outgoing syslog messages
*A:dut-a>config>python>py-policy$ syslog
- syslog script <name>
- no syslog
<name> : [32 chars max]
```

The detailed Python policy description is explained in the “Python Script Support for ESM” section in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*.

### 2. Log filters identify the events that are subject to Python processing

```
A:dut-a>config>log# info
-----
      filter 6
        default-action drop
        entry 1
          action forward
          match
            application eq "nat"
```

```

        number eq 2012
    exit
exit
filter 7
    default-action forward
    entry 1
        action drop
        match
            application eq "nat"
            number eq 2012
        exit
    exit
exit

```

### 3. Syslog destination

```

syslog 1
    address 192.168.1.1
exit

```

### 4. Applying Python syslog policy to selected events via filter 6:

```

log-id 33  Note: Process log events with id of 2012 with Python before
sending them to syslog server.
    filter 6
    from main
    to syslog 1
    python-policy "PyForLogEvents"
    no shutdown
exit
log-id 34  Note: Log events that are not processed by Python.
    filter 7
    from main
    to syslog 1
    no shutdown
exit

```

In the example above, the configuration-only event 2012 from application "nat" will be sent to log-id 33. All other events are forwarded to the same syslog destination via log-id 34, without any modification. As a result, all events (modified via log-id 33 and unmodified via log-id 34) are sent to the syslog 1 destination.

This configuration may cause reordering of syslog messages at the syslog 1 destination due to slight delay of messages processed by Python.

## 6.4.5 Modifying a Log File

The following displays the current log configuration:

```
ALA-12>config>log>log-id# info
```

```

-----
...
log-id 2
    description "This is a test log file."
    filter 1
    from main security
    to file 1

exit
...
-----
ALA-12>config>log>log-id#

```

The following displays an example to modify log file parameters:

```

Example:config# log
config>log# log-id 2
config>log>log-id# description "Chassis log file."
config>log>log-id# filter 2
config>log>log-id# from security
config>log>log-id# exit

```

The following displays the modified log file configuration:

```

A:ALA-12>config>log# info
-----
...
log-id 2
    description "Chassis log file."
    filter 2
    from security
    to file 1

exit
...
-----
A:ALA-12>config>log#

```

## 6.4.6 Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, **file 1** is associated with **log-id 2**.

```

A:ALA-12>config>log# info
-----
file-id 1
    description "LocationTest."
    location cf1:
    rollover 600 retention 24

exit
...
log-id 2
    description "Chassis log file."
    filter 2

```

```

        from security
        to file 1
exit
...
-----
A:ALA-12>config>log#

```

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

```

## 6.4.7 Modifying a File ID

The following displays the current log configuration:

```

A:ALA-12>config>log# info
-----
file-id 1
description "This is a log file."
location cf1:
rollover 600 retention 24
exit
-----
A:ALA-12>config>log#

```

The following displays an example to modify log file parameters:

```

Example:config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit

```

The following displays the file modifications:

```

A:ALA-12>config>log# info
-----
...
file-id 1
description "LocationTest."
rollover 2880 retention 500
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#
```

## 6.4.8 Modifying a Syslog ID

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#
```

## 6.4.9 Modifying an SNMP Trap Group

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#
```

## 6.4.10 Deleting an SNMP Trap Group

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
```

## 6.4.11 Modifying a Log Filter

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#

```

## 6.4.12 Modifying Event Control Parameters

The following displays the current event control configuration:

```

A:ALA-12>config>log# info
-----
...
event-control "bgp" 2014 generate critical
...
-----
A:ALA-12>config>log#

```

The following displays an example of an event control modification:

```

Example:config# log
config>log# event-control bgp 2014 suppress

```

The following displays the log filter configuration:

```

A:ALA-12>config>log# info
-----
...
event-control "bgp" 2014 suppress
...
-----
A:ALA-12>config>log#

```

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 modification:

```
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#
```

## 6.4.13 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:

```
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 "bgp" 2001
config>log# no event-control "bgp" 2002
config>log# no event-control "bgp" 2014

A:ALA-12>config>log# info detail
-----
#-----
echo "Log Configuration"
#-----
event-control "bgp" 2001 generate minor
event-control "bgp" 2002 generate warning
event-control "bgp" 2003 generate warning
event-control "bgp" 2004 generate critical
event-control "bgp" 2005 generate warning
event-control "bgp" 2006 generate warning
event-control "bgp" 2007 generate warning
```

---

```
event-control "bgp" 2008 generate warning
event-control "bgp" 2009 generate warning
event-control "bgp" 2010 generate warning
event-control "bgp" 2011 generate warning
event-control "bgp" 2012 generate warning
event-control "bgp" 2013 generate warning
event-control "bgp" 2014 generate warning
event-control "bgp" 2015 generate critical
event-control "bgp" 2016 generate warning
...
-----
A:ALA-12>config>log#
```

## 6.5 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.

### 6.5.1 Accounting Records

An accounting policy must define a record name and collection interval. Only one record name can be configured per accounting policy. Also, a record name can only be used in one accounting policy.

The record name, sub-record types, and default collection period for service and network accounting policies are shown in [Table 85](#). [Table 87](#) (fields per policer stat-mode are given in the **stat-mode** command descriptions in the *Quality of Service Guide*), [Table 88](#), and [Table 89](#) provide field descriptions.

**Table 85 Accounting Record Name and Collection Periods**

Record Name	Sub-Record Types	Accounting Object	Platform	Default Collection Period (minutes)
service-ingress-octets	sio	SAP	All	5
service-egress-octets	seo	SAP	All	5
service-ingress-packets	sip	SAP	All	5
service-egress-packets	sep	SAP	All	5
network-ingress-octets	nio	Network port	All	15
network-egress-octets	neo	Network port	All	15
network-egress-packets	nep	Network port	All	15
network-ingress-packets	nio	Network port	All	15
compact-service-ingress-octets	ctSio	SAP	All	5
combined-service-ingress	cmSipo	SAP	All	5

**Table 85 Accounting Record Name and Collection Periods (Continued)**

Record Name	Sub-Record Types	Accounting Object	Platform	Default Collection Period (minutes)
combined-network-ing-egr-octets	cmNio & cmNeo	Network port	All	15
combined-service-ing-egr-octets	cmSio & cmSeo	SAP	All	5
complete-network-ingr-egr	cpNipo & cpNepo	Network port	All	15
complete-service-ingress-egress	cpSipo & cpSepo	SAP	All	5
combined-sdp-ingress-egress	cmSdpipo and cmSdpepo	SDP and SDP binding	All	5
complete-sdp-ingress-egress	cmSdpipo, cmSdpepo, cpSdpipo and cpSdpepo	SDP and SDP binding	All	5
complete-subscriber-ingress-egress	cpSBipo & cpSBepo	Subscriber profile	7750 SR	5
aa-protocol	aaProt	AA ISA Group	7750 SR	15
aa-application	aaApp	AA ISA Group	7750 SR	15
aa-app-group	aaAppGrp	AA ISA Group	7750 SR	15
aa-subscriber-protocol	aaSubProt	Special study AA subscriber	7750 SR	15
aa-subscriber-application	aaSubApp	Special study AA subscriber	7750 SR	15
custom-record-aa-sub	aaSubCustom	AA subscriber	All	15
combined-mpls-lsp-egress	mplsLspEgr	LSP	All	5
combined-mpls-lsp-ingress	mplsLspIn	LSP	All	5
saa	saa png trc hop	SAA or SAA test	All	5
complete-ethernet-port	enet	Ethernet port	All	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 *Multiservice Integrated Services Adapter Guide* for fields names for Application Assurance records.

The availability of the records listed in [Table 86](#) depends on the specific platform functionality and user configuration.

**Table 86 Accounting Record Name Details**

Record Name	Sub-Record	Field	Field Description
Service-ingress-octets (sio) <sup>1</sup>	sio	svc	Svcld
		sap	Sapld
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
Service-egress-octets (seo) <sup>1</sup>	seo	svc	Svcld
		sap	Sapld
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 86**      **Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Service-ingress-packets (sip) <sup>1, 2</sup>	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) <sup>1, 2</sup>	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

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
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
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

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
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 86 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

**Table 86      Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Combined-service-ingr-egr-octets (cmSio & CmSeo)	cmSio	svc	Svcld
		sap	Sapld
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
	cmSeo	svc	Svcld
		sap	Sapld
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 86 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 86      Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-service-ingress-egress (cpSipo & cpSepa)	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
		apo	AllPacketsOffered
		aoo	AllOctetsOffered
		apd	AllPacketsDropped
		aod	AllOctetsDropped
		apf	AllPacketsForwarded
		aof	AllOctetsForwarded
		ipd	InProfilePktsDropped
		iod	InProfileOctetsDropped
		opd	OutOfProfilePktsDropped
		ood	OutOfProfileOctetsDropped
		hpf	HighPriorityPacketsForwarded
		hof	HighPriorityOctetsForwarded



**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-service-ingress-egress (cpSipo & cpSepo) (Continued)	cpSipo (Continued)	lpf	LowPriorityPacketsForwarded
		lof	LowPriorityOctetsForwarded
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
	cpSepo	svc	SvcId
		sap	SapId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
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 86      Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Combined-sdp-ingress-egress (cmSdpipo & cmSdpepo)	cmSdpipo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tpd	TotalPacketsDropped
		tof	TotalOctetsForwarded
		tod	TotalOctetsDropped
	cmSdpepo	svc	SvcID
		sdp	SdpID
		tpf	TotalPacketsForwarded
		tof	TotalOctetsForwarded

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
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
Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) <sup>3</sup>	SubscriberInform ation	subId	SubscriberId
		subProfile	SubscriberProfile
	Sla- Information <sup>4</sup>	svc	SvcId
		sap	SapId
		slaProfile	SlaProfile
		spiSharing	SPI sharing type and identifier

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) <sup>3</sup> (Continued)	cpSBipo	qid	QueueId
		hpo	HighPktsOffered <sup>4</sup>
		hpd	HighPktsDropped
		lpo	LowPktsOffered <sup>4</sup>
		lpd	LowPktsDropped
		ucp	UncolouredPacketsOffered
		hoo	OfferedHiPrioOctets <sup>4</sup>
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered <sup>4</sup>
		lod	LowOctetsDropped
		apo	AllPktsOffered <sup>4</sup>
		aoo	AllOctetsOffered <sup>4</sup>
		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

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) <sup>3</sup> (Continued)	cpSBepo	qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped
		v4pf	IPv4PktsForwarded
		v6pf	IPv6PktsForwarded
		v4pd	IPv4PktsDropped
		v6pd	IPv6PktsDropped
		v4of	IPv4OctetsForwarded
		v6of	IPv6OctetsForwarded
		v4od	IPv4OctetsDropped
		v6od	IPv6OctetsDropped

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
Complete-subscriber-ingress-egress (cpSBipo & cpSBepo) (cpSBipooc & cpSBepooc) <sup>3</sup> (Continued)	cpSBipooc <sup>3</sup>	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 <sup>3</sup>	cid	OverrideCounterId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		ofp	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		ipd	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

**Table 86 Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
saa	saa	tmd	TestMode
		own	OwnerName
		tst	TestName
		png	PingRun subrecord
		rid	RunIndex
		trr	TestRunResult
		mnr	MinRtt
		mrx	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

**Table 86      Accounting Record Name Details (Continued)**

Record Name	Sub-Record	Field	Field Description
saa (Continued)	trc	rid	RunIndex
		trr	TestRunResult
		lgp	LastGoodProbe
	hop	hop	TraceHop
		hid	HopIndex
		mnr	MinRtt
		mrx	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 86 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	EtherStatsCRCAAlignErrors
		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

**Table 86** Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Complete-ethernet-port (enet) (Continued)	enet (Continued)	lcc	Dot3StatsLateCollisions
		exc	Dot3StatsExcessiveCollisions
		imt	Dot3StatsInternalMacTransmitErrors
		cse	Dot3StatsCarrierSenseErrors
		ftl	Dot3StatsFrameTooLongs
		imre	Dot3StatsInternalMacReceiveErrors
		se	Dot3StatsSymbolErrors
		ipf	Dot3InPauseFrames
		opf	Dot3OutPauseFrames

## Notes:

1. 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.
2. 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.
3. If override counters on the HSMDA are configured (see the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR Quality of Service Guide*).
4. 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 87](#), [Table 88](#), and [Table 89](#) provide field descriptions.

**Table 87** Policer Stats Field Descriptions

Field	Field Description
pid	PolicerId
statmode	PolicerStatMode
aod	AllOctetsDropped
aof	AllOctetsForwarded
aoo	AllOctetsOffered
apd	AllPacketsDropped

**Table 87 Policer Stats Field Descriptions (Continued)**

Field	Field Description
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
oof	OutOfProfileOctetsForwarded
ooo	OutOfProfileOctetsOffered
xpd	ExceedProfilePktsDropped

**Table 87**      **Policer Stats Field Descriptions (Continued)**

Field	Field Description
xpf	ExceedProfilePktsForwarded
xpo	ExceedProfilePktsOffered
xod	ExceedProfileOctetsDropped
xof	ExceedProfileOctetsForwarded
xoo	ExceedProfileOctetsOffered
ppd	InplusProfilePacketsDropped
ppf	InplusProfilePacketsForwarded
ppo	InplusProfilePacketsOffered
pod	InplusProfileOctetsDropped
pod	InplusProfileOctetsDropped
pof	InplusProfileOctetsForwarded
poo	InplusProfileOctetsOffered
uco	UncoloredOctetsOffered
ucp	UncoloredPacketsOffered
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 88 Queue Group Record Types**

Record Name	Description
qgone	PortQueueGroupOctetsNetworkEgress
qgosi	PortQueueGroupOctetsServiceIngress
qgose	PortQueueGroupOctetsServiceEgress
qgpne	PortQueueGroupPacketsNetworkEgress
qgpsi	PortQueueGroupPacketsServiceIngress
qgpse	PortQueueGroupPacketsServiceEgress
fpqgosi	ForwardingPlaneQueueGroupOctetsServiceIngress
fpqgoni	ForwardingPlaneQueueGroupOctetsNetworkIngress
fpqgpsi	ForwardingPlaneQueueGroupPacketsServiceIngress
fpqgpni	ForwardingPlaneQueueGroupPacketsNetworkIngress

**Table 89 Queue Group Record Type Fields**

Field	Field Description
data port	Port (used for port based Queue Groups)
member-port	LAGMemberPort (used for port based Queue Groups)
data slot	Slot (used for Forwarding Plane based Queue Groups)
forwarding-plane	ForwardingPlane (used for Forwarding Plane based Queue Groups)
queue-group	QueueGroupName
instance	QueueGroupInstance
qid	QueueId
pid	PolicerId
statmode	PolicerStatMode
aod...ucp	same as above

## 6.5.2 Accounting Files

When a policy has been created and applied to a service or network port, the accounting file is stored on the compact flash in a compressed XML file format. The 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](#).

## 6.5.3 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.

## 6.5.4 Reporting and Time-Based Accounting

SR OS on the 7750 SR platform has support for volume accounting and time-based accounting concepts, and 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 compares 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.

## 6.5.5 Overhead Reduction in Accounting: Custom Record

Custom records can be used to decrease accounting messaging overhead as follows:

- [User Configurable Records](#)
- [Changed Statistics Only](#)
- [Configurable Accounting Records](#)
- [Significant Change Only Reporting](#)

### 6.5.5.1 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.

### 6.5.5.2 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).

### 6.5.5.3 Configurable Accounting Records

#### 6.5.5.3.1 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.

ESM-based accounting applies to the 7750 SR only.

Record headers including information such as service-ID, SAP-ID, and so on, will always be generated.

#### 6.5.5.3.2 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. This functionality applies to the 7750 SR only.

### 6.5.5.4 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.

## 6.5.6 Immediate Completion of Records

### 6.5.6.1 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. This functionality applies to the 7750 SR only.

## 6.5.7 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.

---

## 6.6 Configuration Notes

This section describes logging configuration restrictions.

- A file or filter cannot be deleted if it has been applied to a log.
- File IDs, syslog IDs, or SNMP trap groups must be configured before they can be applied to a log ID.
- A file ID can only be assigned to *either* one log ID *or* one accounting policy.
- Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.
- The **snmp-trap-id** must be the same as the **log-id**.

## 6.7 Configuring Logging with CLI

This section provides information to configure logging with the command line interface.

### 6.7.1 Log Configuration Overview

Configure logging parameters to save information in a log file or direct the messages to other devices. Logging does the following:

- Provides you with logging information for monitoring and troubleshooting.
- Allows the selection of the types of logging information to be recorded.
- Allows the assignment of a severity to the log messages.
- Allows the selection of source and target of logging information.

### 6.7.2 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 or 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.

## 6.7.3 Basic 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 for the 7750 SR.

```
A:ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
    event-control "bgp" 2001 generate critical
    file-id 1
        description "This is a test file-id."
        location cf1:
    exit
    file-id 2
        description "This is a test log."
        location cf1:
    exit
    snmp-trap-group 7
        trap-target 11.22.33.44 "snmpv2c" notify-community "public"
    exit
    log-id 2
        from main
        to file 2
    exit
-----
A:ALA-12>config>log#
```

## 6.7.4 Common Configuration Tasks

The following sections describe basic system tasks that must be performed.

### 6.7.4.1 Configuring an Event Log

A event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

```
config>log
      log-id log-id
      description description-string
      filter filter-id
      from {[main] [security] [change] [debug-trace]}
      to console
      to file file-id
      to memory [size]
      to session
      to snmp [size]
      to syslog syslog-id}
      time-format {local | utc}
      no shutdown
```

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#
```

### 6.7.4.2 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.

When creating new log files in a compact flash disk card, the minimum amount of free space is the MINIMUM of 10% of Compact Flash disk capacity OR 5 Mb (5,242,880 = 5 \* 1024 \* 1024).

The following displays a log file configuration example:

```
A:ALA-12>config>log# info
-----
      file-id 1
      description "This is a log file."
      location cf1:
      rollover 600 retention 24
```

```
exit
-----
A:ALA-12>config>log#
```

6.7.4.3 Configuring an Accounting Policy

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory of compact flash (cf1: or cf2:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See [Configuring an Event Log](#) and [Configuring a File ID](#).

Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one 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.

By default, the subscriber host volume accounting data are based on the 14-byte Ethernet DLC header, 4-byte or 8-byte VLAN Tag (optional), 20-byte IP header, IP payload, and the 4-byte CRC (everything except the preamble and inter-frame gap). See [Figure 20](#). This default can be altered by the **packet-byte-offset** configuration option.

Figure 20 Subscriber Host Volume Accounting Data

Destination MAC	Source MAC	802.1Q tag (optional)	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	CRC/FCS
6 octets	6 octets	(4 octets)	(4 octets)	2 octets	46-1500 octets	4 octets

0971

The following displays an 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
```

### 6.7.4.4 Configuring Event Control

The following displays an example of 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#
```

### 6.7.4.5 Configuring a Log Filter

The following displays a log filter configuration example:

```
A:ALA-12>config>log# info
#-----
echo "Log Configuration "
#-----
        file-id 1
            description "This is our log file."
            location cf1:
            rollover 600 retention 24
        exit
        filter 1
            default-action drop
            description "This is a sample filter."
            entry 1
                action forward
                match
                    application eq "mirror"
                    severity eq critical
            exit
        exit
    ...
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#

```

### 6.7.4.6 Configuring an SNMP Trap Group

The associated *log-id* does not have to be configured before a **snmp-trap-group** can be created, however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

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 "communitystring"
    exit
...
log-id 2
        description "This is a test log file."
        filter 1
        from main security
        to file 1
    exit
...
-----
A:ALA-12>config>log#

```

The following displays a SNMP trap group, log, and interface configuration examples:

```

A:SetupCLI>config>log# snmp-trap-group 44
A:SetupCLI>config>log>snmp-trap-group# info
-----
        trap-target "xyz-test" address xx.xx.x.x snmpv2c notify-community "xyztesting"
        trap-target "test2" address xx.xx.xx.x snmpv2c notify-community "xyztesting"
-----
*A:SetupCLI>config>log>log-id# info
-----
        from main
        to snmp
-----
*A:SetupCLI>config>router# interface xyz-test
*A:SetupCLI>config>router>if# info
-----
        address xx.xx.xx.x/24

```



```

        port 1/1/1
-----
*A:SetupCLI>config>router>if#

```

#### 6.7.4.6.1 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 10.20.20.5 snmpv2c notify-community "xyztesting"
-----
A:SetupCLI>config>log>snmp-trap-group#

```

In the following output, 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    : 10.20.20.5
Port      : 162
Version   : v2c
Community  : xyztesting
Sec. Level : none
Replay    : disabled
Replay from : n/a
Last replay : never
=====
A:SetupCLI>config>log>snmp-trap-group#

```

Since no events are waiting to be replayed, the log displays as before.

```

A:SetupCLI>config>log>snmp-trap-group# show log log-id 44
=====
Event Log 44
=====

```

```

SNMP Log contents [size=100  next event=3819  (wrapped)]

3818 2008/04/22 23:35:39.89 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed
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

```

#### 6.7.4.6.2 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    : 10.20.20.5
Port       : 162
Version    : v2c
Community  : xyztesting
Sec. Level : none
Replay     : disabled
Replay from : n/a
Last replay : never
=====
*A:SetupCLI#
```

A display of the event log indicates which trap targets are not accessible and waiting for notification replay and the sequence ID of the first notification that will be replayed.



**Note:** 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 Nokia 7750 SR Copyright (c)
2000-2016 Nokia. 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"
```

### 6.7.4.6.3 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    : 10.20.20.5
Port       : 162
Version    : v2c
Community  : xyztesting
Sec. Level : none
Replay     : disabled
Replay from : n/a
Last replay : never
=====
*A:SetupCLI#
```

A display of the event log shows that it is no longer waiting to replay notifications to one or more of its trap target addresses. An event message has been written to the logger that indicates the replay to the trap-target address has happened and displays the notification sequence ID of the first and last replayed notifications.

```
*A:SetupCLI# show log log-id 44
=====
Event Log 44
=====
SNMP Log contents [size=100 next event=3827 (wrapped)]
```

```
3826 2008/04/22 23:42:02.15 UTC MAJOR: LOGGER #2015 Base Log-id 44
"Missed events 3819 to 3825 from Log-id 44 have been resent to SNMP notification
target address 10.10.10.3."

3825 2008/04/22 23:42:02.15 UTC INDETERMINATE: LOGGER #2011 Base Event Test
"Test event has been generated with system object identifier tmnxModelSR12Reg.
System description: TiMOS-B-0.0.private both/i386 Nokia 7750 SR Copyright (c)
2000-2016 Nokia.
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 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"
```

## 6.7.4.7 Configuring a Syslog Target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

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#
```

### 6.7.4.7.1 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  
-----





## 6.8 Log Configuration Command Reference

This section provides the log configuration command reference.

### 6.8.1 Command Hierarchies

- [Log Configuration Command Reference](#)
  - [Log Configuration Commands](#)
  - [Accounting Policy Commands](#)
  - [Custom Record Commands](#)
  - [File ID Commands](#)
  - [Event Filter Commands](#)
  - [Event Handling System \(EHS\) Commands](#)
  - [Event Trigger Commands](#)
  - [Log ID Commands](#)
  - [SNMP Trap Group Commands](#)
  - [Syslog Commands](#)
  - [Show Commands](#)
  - [Clear Command](#)

#### 6.8.1.1 Log Configuration Commands

```

config
— log
— app-route-notifications
    — cold-start-wait seconds
    — no cold-start-wait
    — route-recovery-wait seconds
    — no route-recovery-wait
— event-control application-id [event-name | event-number] [generate] [severity-level]
    [throttle] [specific-throttle-rate events-limit interval seconds | disable-specific-
    throttle] [repeat | no-repeat]
— event-control application-id [event-name | event-number] suppress
— no event-control application-id [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

```

### 6.8.1.2 Accounting Policy Commands

```

config
  — log
    — accounting-policy acct-policy-id
    — no accounting-policy acct-policy-id
      — collection-interval minutes
      — no collection-interval
      — [no] default
      — description description-string
      — no description
      — [no] include-system-info
      — record record-name
      — no record
      — [no] shutdown
      — to file log-file-id

```

### 6.8.1.3 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-attributes [all]
          — no aa-sub-attributes
            — [no] app-profile
            — [no] app-service-options
          — aa-sub-counters [all]
          — no aa-sub-counters
            — all
            — [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-timestamp
            — [no] octets-admitted-count

```

- [no] octets-denied-count
  - [no] packets-admitted-count
  - [no] packets-denied-count
- to-aa-sub-counters [all]
- no 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-timestamp
  - [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] all-octets-offered-count
    - [no] all-packets-offered-count
    - [no] high-octets-discarded-count
    - [no] high-packets-discarded-count
    - [no] in-profile-octets-forwarded-count
    - [no] in-profile-packets-forwarded-count
    - [no] low-octets-discarded-count
    - [no] low-packets-discarded-count
    - [no] out-profile-octets-forwarded-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-octets-offered-count**
  - [no] **low-packets-discarded-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-packets-discarded-count**
      - [no] **in-profile-octets-forwarded-count**
      - [no] **in-profile-packets-forwarded-count**
      - [no] **low-octets-discarded-count**
      - [no] **low-packets-discarded-count**
      - [no] **out-profile-octets-forwarded-count**
      - [no] **out-profile-packets-forwarded-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
  - [no] uncoloured-octets-offered-count
  - [no] uncoloured-packets-offered-count
- significant-change *delta*
- no significant-change

#### 6.8.1.4 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
  
```

#### 6.8.1.5 Event Filter Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* 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**

### 6.8.1.6 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
          — min-delay [delay]
          — no min-delay
          — script-policy policy-name [owner owner-name]
          — no script-policy
          — [no] shutdown
        — description description-string
        — no description
        — [no] shutdown

```

### 6.8.1.7 Event Trigger Commands

- ```

config
  — log
    — event-trigger
      — [no] event application-id event-name-id
        — description description-string
        — no description
        — [no] shutdown
      — [no] trigger-entry entry-id
        — debounce occurrences [within seconds]
        — no debounce

```

- **event-handler** *event-handler*
- [no] **event-handler**
- **description** *description-string*
- **no description**
- **log-filter** *filter-id*
- [no] **log-filter**
- [no] **shutdown**

### 6.8.1.8 Log ID Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* 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
      — netconf-stream stream-name
      — no netconf-stream
      — python-policy policy-name
      — no python-policy
      — [no] shutdown
      — time-format {local | utc}
      — to cli [size]
      — to console
      — to file log-file-id
      — to memory [size]
      — to netconf [size]
      — to session
      — to snmp [size]
      — to syslog syslog-id

```

### 6.8.1.9 SNMP Trap Group Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* 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*

### 6.8.1.10 Syslog Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* 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 level
      — no level
      — log-prefix log-prefix-string
      — no log-prefix
      — port port
      — no port

```

## 6.8.2 Command Descriptions

- [Generic Commands](#)
- [Log Configuration Commands](#)
- [Custom Record Commands](#)
- [File ID Commands](#)
- [Event Filter Commands](#)
- [Event Handling System \(EHS\) Commands](#)
- [Event Trigger Commands](#)
- [Syslog Commands](#)
- [SNMP Trap Groups](#)
- [Accounting Policy Commands](#)



## 6.8.2.1 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, and so on), 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-handling>handler>entry config>log>event-trigger>event config>log>event-trigger>event>trigger-entry
<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.

<b>Default</b>	no shutdown
<b>Parameters</b>	<p><i>log-id log-id</i> — When a <i>log-id</i> is shut down, no events are collected for the entity. This leads to the loss of event data.</p> <p><i>accounting-policy accounting Policy</i> — 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 (<b>no shutdown</b>) the counters include the data collected during the period the policy was shut down.</p>

## 6.8.2.2 Log Configuration Commands

### app-route-notifications

<b>Syntax</b>	<b>app-route-notifications</b>
<b>Context</b>	config>log
<b>Description</b>	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 <i>route available</i> or <i>route changed</i> 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

<b>Syntax</b>	<b>cold-start-wait seconds</b> <b>no cold-start-wait</b>
<b>Context</b>	config>log>app-route-notifications
<b>Description</b>	The time delay that must pass before notifying specific CPM applications that a route is available after a cold reboot.
<b>Default</b>	no cold-start-wait
<b>Parameters</b>	<i>seconds</i> — time delay in seconds
<b>Values</b>	1 to 300

## route-recovery-wait

<b>Syntax</b>	<b>route-recovery-wait</b> <i>seconds</i> <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>	<i>seconds</i> — time delay in seconds <b>Values</b> 1 to 100

## 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> ] [ <i>throttle</i> ] [ <b>specific-throttle-rate</b> <i>events-limit interval seconds</i>   <b>disable-specific-throttle</b> ] [ <b>repeat</b>   <b>no-repeat</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-id</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 <a href="#">event-control</a> command.

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

**Values**            A valid application name. To display a list of valid application names, use the **show log applications** command.

Some examples of valid applications are:

```
application_assurance|aps|atm|auto_prov|bfd|bgp|bier|
bmp|calltrace|ccag|cflowd|chassis|cpmhfilter|
cpmhqueue|debug|dhcp|dhcps|diameter|dot1x|dynsvc|
efm_oam|elmi|ering|eth_cfm|etun|filter|fpe|gsm|gmps|
gtp|gtungrp|icl|igh|igmp|igmp_snooping|ip|ipfix|ipsec|
ipsec_cpm|isis|l2tp|lag|ldap|ldp|li|lldp|lmp|logger|
macsec|mcac|mcp|mcpath|mc_redundancy|mgmt_core|mirror|mld|
mld_snooping|mpls|mpls_tp|mpls_lm|mrp|msdp|nat|nge|
ntp|oam|open_flow|ospf|pcap|pcep|pfc|pim|
pim_snooping|port|ppp|pppoe|pppoe_clnt|profile|ptp|
pxc|python|qos|radius|rip|rip_ng|route_next_hop|
route_policy|rpki|rsdp|security|sflow|snmp|sr_policy|
stp|subscr_mgmt|sub_host_trk|svcmgr|system|tip|tls|
user|user_db|video|vrrp|vrtr|wlan_gw|wpp
```

**Default**            None, this parameter must be explicitly specified.

*event-name* — To generate, suppress, or revert to default for a single event, enter the specific event short name. If no event 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**            Up to 32 characters

*event-number* — To generate, suppress, or revert to default for a single event, enter the specific number. If no event number is specified, the command applies to all events in the application.

**Default**            none

**Values**            0 to 4294967295

*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-level* — An ASCII string representing the severity level to associate with the specified generated events

**Default**            The system assigned severity name

**Values**            One of: cleared, indeterminate, critical, major, minor, warning.

**throttle** — Specifies whether or not events of this type will be throttled. By default, event throttling is on for most event types.

**suppress** — This keyword indicates that the specified events will not be logged. If the **suppress** keyword is not specified then the events are generated by default. For example on the 7750 SR, **event-control bgp suppress** will suppress all BGP events. If a log event is a raising event for a Facility Alarm, and the associated Facility Alarm is raised, then changing the log event to **suppress** clears the associated Facility Alarm.

**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 to 20000

**interval seconds** — specifies the number of seconds that the specific throttling intervals lasts.

**Values** 1 to 1200

**disable-specific-throttle** — Specifies to disable the **specific-throttle-rate**.

**repeat** — Specifies that the log event should be repeated every minute until the underlying condition is cleared. Only supported for the following log events: BGP tBgpMaxNgPfxLmtThresholdReached and PORT tmnxEqPortEtherCrcAlarm (for **degrade** threshold only)

## event-damping

<b>Syntax</b>	<b>[no] event-damping</b>
<b>Context</b>	config>log
<b>Description</b>	This command allows the user to set the event damping algorithm to suppress QoS or filter change events.



**Note:** While this event damping is original behavior for some modules such as service manager, QoS, and filters, it can result in the NMS system database being out of sync because of missed change events. On the other hand, if the damping is disabled (**no event-damping**), it may take much longer to **exec** a large CLI configuration file after system bootup.

## 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>

## throttle-rate

<b>Syntax</b>	<b>throttle-rate</b> <i>events</i> [ <i>interval seconds</i> ] <b>no throttle-rate</b>
<b>Context</b>	config>log
<b>Description</b>	This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the <b>event-control</b> command and do not have a <b>specific-throttle-rate</b> configured.
<b>Default</b>	throttle-rate 2000 interval 1

<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 to 20000</p>
	<p><b>Default</b> 2000</p>
	<p><i>interval seconds</i> — Specifies the number of seconds that an event throttling interval lasts.</p>
	<p><b>Values</b> 1 to 1200</p>
	<p><b>Default</b> 1</p>

### 6.8.2.3 Accounting Policy Commands

#### accounting-policy

<b>Syntax</b>	<p><b>accounting-policy</b> <i>policy-id</i> [interval minutes] <b>no accounting-policy</b> <i>policy-id</i></p>
<b>Context</b>	<p>config&gt;log</p>
<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>

If no accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy as designated with the **default** command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured. Default accounting policies cannot be explicitly applied. For example, for **accounting-policy 10**, if default is set, then that policy cannot be used:

```
*A:75>config>service>vpls>spoke-sdp# accounting-policy 10
```

Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new network default policy can be configured.

The **no** form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.

<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 to 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 to 120 A range of 1 to 4 is only allowed when the record type is set to SAA.

default

<b>Syntax</b>	<b>[no] default</b>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.



If no access accounting policy is defined on a SAP, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

If no network accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one access accounting policy ID can be designated as the default access policy. Likewise, only one network accounting policy ID can be designated as the default network accounting policy.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of the command removes the default policy designation from the policy ID. The accounting policy will be removed from all SAPs or network ports that do not have this policy explicitly defined.

## 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-system-info

## record

<b>Syntax</b>	<b>[no] record</b> <i>record-name</i>
<b>Context</b>	config>log>accounting-policy
<b>Description</b>	<p>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 <b>show log accounting-records</b> command.</p>



**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:** 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 record

**Parameters** *record-name* — Specifies the accounting record name. [Table 90](#) lists the accounting record names available and the default collection interval.

**Table 90** Default Collection Interval for Accounting Records

Record Type	Accounting Record Name	Default Interval
1	service-ingress-octets	5

**Table 90**      **Default Collection Interval for Accounting Records (Continued)**

Record Type	Accounting Record Name	Default Interval
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

**Table 90 Default Collection Interval for Accounting Records (Continued)**

Record Type	Accounting Record Name	Default Interval
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	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
<b>Description</b>	This command specifies the destination for the accounting records selected for the accounting policy.
<b>Default</b>	No destination is specified.
<b>Parameters</b>	<i>file-id</i> — Specifies the destination for the accounting records selected for this destination. The characteristics of the file ID must have already been defined in the <b>config&gt;log&gt;file</b> context. A file ID can only be used once. The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics. If the <b>to</b> command is executed while the accounting policy is in operation, then it becomes active during the next collection interval. <b>Values</b> 1 to 99

#### 6.8.2.3.1 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>	collection-interval 5
<b>Parameters</b>	<i>minutes</i> — Specifies the collection interval in minutes. <b>Values</b> 5 to 120

custom-record

<b>Syntax</b>	<b>[no] custom-record</b>
<b>Context</b>	config>log>acct-policy

---

**Description** This command enables the context to configure the layout and setting for a custom accounting record associated with this accounting policy.

The **no** form of the command reverts the configured values to the defaults.

## aa-specific

**Syntax** [no] **aa-specific**

**Context** config>log>acct-policy>cr

**Description** This command enables the context to configure information for this custom record.

The **no** form of the command excludes aa-specific attributes in the AA subscriber's custom record.

## override-counter

**Syntax** [no] **override-counter** *override-counter-id*

**Context** config>log>acct-policy>cr

**Description** This command enables the context to configure override counter (HSMDA) parameters. This command only applies to the 7750 SR.

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

**Parameters** *override-counter-id* — Specifies the override counter ID.

**Values** 1 to 8

## queue

**Syntax** [no] **queue** *queue-id*

**Context** config>log>acct-policy>cr

**Description** This command specifies the queue-id for which counters will be collected in this custom record. The counters that will be collected are defined in egress and ingress counters.

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

**Parameters** *queue-id* — Specifies the queue-id for which counters will be collected in this custom record.

---

## 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>	<p>This command enables the use of significant-change so only those aa-specific records which have changed in the last accounting interval are written.</p> <p>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.</p>
<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</b> <i>ref-override-counter-id</i> <b>ref-override-counter all</b> <b>no ref-override-counter</b>
<b>Context</b>	config>log>acct-policy>cr
<b>Description</b>	<p>This command configures a reference override counter.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>
<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>	<p>This command configures a reference queue.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>
<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 to 4294967295 (For custom-record-aa-sub only values 0 or 1 are supported.)

## aa-sub-attributes

<b>Syntax</b>	<b>aa-sub-attributes</b> [all] <b>no aa-sub-attributes</b>
<b>Context</b>	config>log>acct-policy>cr>aa
<b>Description</b>	This command enables the context to configure aa-specific attributes such as aa-sub-attributes and counters that will be available in the AA subscriber's custom record.  The <b>no</b> form of the command excludes aa specific attributes from the AA subscriber's custom record.
<b>Parameters</b>	<b>all</b> — Specifies all counters.

## app-profile

<b>Syntax</b>	[no] <b>app-profile</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-attributes
<b>Description</b>	This command enables the subscriber app-profile attribute information to be exported in the AA subscriber's custom record.  The <b>no</b> form of the command excludes the subscriber app-profile attribute from the AA subscriber's custom record.

## app-service-options

<b>Syntax</b>	[no] <b>app-service-options</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-attributes

- 
- Description** This command enables the subscriber application service option attributes to be exported in the AA subscriber's custom record.
- The **no** form of the command excludes the subscriber application service option attributes from the AA subscriber's custom record.

## aa-sub-counters

- Syntax** **aa-sub-counters [all]**  
**no aa-sub-counters**
- Context** config>log>acct-policy>cr>aa
- Description** This command enables the context to configure subscriber counter information. This command only applies to the 7750 SR.
- The **no** form of the command excludes the aa-sub-counters attributes in the AA subscriber's custom record.
- Parameters** **all** — Specifies all counters.

## from-aa-sub-counters

- Syntax** **[no] from-aa-sub-counters [all]**
- Context** config>log>acct-policy>cr>aa
- Description** This command enables the context to configure Application Assurance “from subscriber” counter parameters. This command only applies to the 7750 SR.
- The **no** form of the command excludes the “from subscriber” count.

## to-aa-sub-counters

- Syntax** **to-aa-sub-counters**  
**no to-aa-sub-counters**
- Context** config>log>acct-policy>cr>aa
- Description** This command enables the context to configure Application Assurance “to subscriber” counter parameters and only applies to the 7750 SR.
- The **no** form of the command excludes the “to subscriber” count.

## long-duration-flow-count

<b>Syntax</b>	<b>[no] long-duration-flow-count</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr
<b>Description</b>	<p>This command includes the long duration flow count. This command only applies to the 7750 SR.</p> <p>The <b>no</b> form of the command excludes the long duration flow count in the AA subscriber's custom record.</p>
<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>	<p>This command includes the medium duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.</p> <p>The <b>no</b> form of the command excludes the medium duration flow count.</p>
<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>	<p>This command includes the short duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.</p> <p>The <b>no</b> form of the command excludes the short duration flow count.</p>
<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>	<p>This command includes the total flow duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.</p>

---

The **no** 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. This command only applies to the 7750 SR.  The <b>no</b> form of the command excludes the total flow duration flow count.

## all

<b>Syntax</b>	<b>all</b>
<b>Context</b>	config>log>acct-policy>cr>aa>aa-sub-cntr 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 include all counters and only applies to the 7750 SR.

## 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 and only applies to the 7750 SR.  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 and only applies to the 7750 SR.

The **no** form of the command excludes the flow's admitted count in the AA subscriber's custom record.

**Default** no flows-admitted-count

## flows-denied-count

**Syntax** [no] flows-denied-count

**Context** config>log>acct-policy>cr>aa>aa-from-sub-cntr  
config>log>acct-policy>cr>aa>aa-to-sub-cntr

**Description** This command includes the flow's denied count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of the command excludes the flow's denied count.

**Default** no flows-denied-count

## forwarding-class

**Syntax** [no] forwarding-class

**Context** config>log>acct-policy>cr>aa>aa-from-sub-cntr  
config>log>acct-policy>cr>aa>aa-to-sub-cntr

**Description** This command enables the collection of a Forwarding Class bitmap information added to the XML aa-sub and router level accounting records, and only applies to the 7750 SR.

**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. This command only applies to the 7750 SR.

The **no** form of the command excludes the maximum throughput octet count.

---

## max-throughput-packet-count

<b>Syntax</b>	<b>[no] max-throughput-packet-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 maximum throughput as measured in the packet count. This command only applies to the 7750 SR.  The <b>no</b> form of the command excludes the maximum throughput packet count.

## max-throughput-timestamp

<b>Syntax</b>	<b>[no] max-throughput-timestamp</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 timestamp of the maximum throughput. This command only applies to the 7750 SR.  The <b>no</b> form of the command excludes the timestamp.

## octets-admitted-count

<b>Syntax</b>	<b>[no] octets-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 octet count in the AA subscriber's custom record and only applies to the 7750 SR.  The <b>no</b> form of the command excludes the admitted octet count.
<b>Default</b>	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 and only applies to the 7750 SR.

The **no** form of the command excludes the denied octet count.

**Default** no octets-denied-count

## packets-admitted-count

**Syntax** [no] packets-admitted-count

**Context** config>log>acct-policy>cr>aa>aa-from-sub-cntr  
config>log>acct-policy>cr>aa>aa-to-sub-cntr

**Description** This command includes the admitted packet count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of the command excludes the admitted packet count.

**Default** no packets-admitted-count

## packets-denied-count

**Syntax** [no] packets-denied-count

**Context** config>log>acct-policy>cr>aa>aa-from-sub-cntr  
config>log>acct-policy>cr>aa>aa-to-sub-cntr

**Description** This command includes the denied packet count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of the command excludes the denied packet count.

**Default** no packets-denied-count

## e-counters

**Syntax** [no] e-counters

**Context** config>log>acct-policy>cr>override-cntr  
config>log>acct-policy>cr>queue  
config>log>acct-policy>cr>ref-override-cntr  
config>log>acct-policy>cr>ref-queue

**Description** This command configures egress counter parameters for this custom record.

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

---

## i-counters

<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>queue 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
```

**Description** This command includes the in-profile packets discarded count.

The **no** form of the command excludes the in-profile packets discarded count.

## in-profile-packets-forwarded-count

**Syntax** [no] in-profile-packets-forwarded-count

**Context** config>log>acct-policy>cr>oc>e-count  
config>log>acct-policy>cr>roc>e-count  
config>log>acct-policy>cr>queue>e-count  
config>log>acct-policy>cr>ref-queue>e-count

**Description** This command includes the in-profile packets forwarded count.

The **no** form of the command excludes the in-profile packets forwarded count.

## out-profile-octets-discarded-count

**Syntax** [no] out-profile-octets-discarded-count

**Context** config>log>acct-policy>cr>oc>e-count  
config>log>acct-policy>cr>roc>e-count  
config>log>acct-policy>cr>queue>e-count  
config>log>acct-policy>cr>ref-queue>e-count

**Description** This command includes the out of profile packets discarded count.

The **no** form of the command excludes the out of profile packets discarded count.

## out-profile-octets-forwarded-count

**Syntax** [no] out-profile-octets-forwarded-count

**Context** config>log>acct-policy>cr>oc>e-count  
config>log>acct-policy>cr>roc>e-count  
config>log>acct-policy>cr>queue>e-count  
config>log>acct-policy>cr>ref-queue>e-count

**Description** This command includes the out of profile octets forwarded count.

The **no** form of the command excludes the out of profile octets forwarded count.

---

## out-profile-packets-discarded-count

<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
```

**Description** This command includes all packets offered in the count.

The **no** form of the command excludes the packets offered in the count.

**Default** no all-packets-offered-count

## high-octets-discarded-count

**Syntax** [no] high-octets-discarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the high octets discarded count.

The **no** form of the command excludes the high octets discarded count.

**Default** no high-octets-discarded-count

## high-octets-offered-count

**Syntax** [no] high-octets-offered-count

**Context** config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the high octets offered count.

The **no** form of the command excludes the high octets offered count.

## high-packets-discarded-count

**Syntax** [no] high-packets-discarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the high packets discarded count.

The **no** form of the command excludes the high packets discarded count.

---

**Default** no high-packets-discarded-count

## high-packets-offered-count

**Syntax** [no] high-packets-offered-count

**Context** config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the high packets offered count.  
The **no** form of the command excludes the high packets offered count.

**Default** no high-packets-offered -count

## in-profile-octets-forwarded-count

**Syntax** [no] in-profile-octets-forwarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the in profile octets forwarded count.  
The **no** form of the command excludes the in profile octets forwarded count.

**Default** no in-profile-octets-forwarded-count

## in-profile-packets-forwarded-count

**Syntax** [no] in-profile-packets-forwarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the in profile packets forwarded count.  
The **no** form of the command excludes the in profile packets forwarded count.

**Default** no in-profile-packets-forwarded-count

## low-octets-discarded-count

<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>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>queue>i-count config>log>acct-policy>cr>ref-queue>i-count

---

**Description** This command includes the low packets discarded count.  
The **no** form of the command excludes the low packets discarded count.

## out-profile-octets-forwarded-count

**Syntax** [no] out-profile-octets-forwarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the out of profile octets forwarded count.  
The **no** form of the command excludes the out of profile octets forwarded count.

**Default** no out-profile-octets-forwarded-count

## out-profile-packets-forwarded-count

**Syntax** [no] out-profile-packets-forwarded-count

**Context** config>log>acct-policy>cr>oc>i-count  
config>log>acct-policy>cr>roc>i-count  
config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the out of profile packets forwarded count.  
The **no** form of the command excludes the out of profile packets forwarded count.

**Default** no out-profile-packets-forwarded-count

## uncoloured-octets-offered-count

**Syntax** [no] uncoloured-packets-offered-count

**Context** config>log>acct-policy>cr>queue>i-count  
config>log>acct-policy>cr>ref-queue>i-count

**Description** This command includes the uncoloured octets offered in the count.  
The **no** form of the command excludes the uncoloured octets offered in the count.

## uncoloured-packets-offered-count

<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.

### 6.8.2.4 File ID Commands

#### file-id

<b>Syntax</b>	<b>[no] file-id <i>file-id</i></b>
<b>Context</b>	config>log
<b>Description</b>	This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.

This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the **to** command under **log-id** or **accounting-policy** to direct specific logging or billing source streams to the file destination.

A file ID can only be assigned to either *one* **log-id** or *one* **accounting-policy**. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.

A file is created when the file ID defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.

The file names for a log are created by the system as summarized in [Table 91](#).

**Table 91 Log File Names**

File Type	File Name
Log File	log/lff-timestamp
Accounting File	actaaff-timestamp

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the file-id
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
  - *yyyy* is the year (for example, 2006)
  - *mm* is the month number (for example, 12 for December)
  - *dd* is the day of the month (for example, 03 for the 3rd of the month)
  - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
  - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
  - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a *gz* extension.

When initialized, each file will contain:

- *The log-id* description.
- *The* time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

<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 to 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, and so on).</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 effect until the log is rolled over either because the rollover period has expired or a <b>clear log log-id</b> 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> <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.</p> <p>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.</p> <p>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.</p> <p>Use the <b>no</b> form of this command to revert to default settings.</p>
<b>Default</b>	Log files are created on cf1: and accounting files are created on cf2:
<b>Parameters</b>	<p><i>cflash-id</i> — Specify the primary location.</p> <p><b>Values</b> cflash-id:cf1:, cf2:, cf3:</p> <p><i>backup-cflash-id</i> — Specify the secondary location.</p> <p><b>Values</b> cflash-id: cf1:, cf2:, cf3:</p>

## rollover

<b>Syntax</b>	<b>rollover</b> <i>minutes</i> [ <i>retention hours</i> ] <b>no rollover</b>
<b>Context</b>	config>log>file-id
<b>Description</b>	This command configures how often an event or accounting log is rolled over or partitioned into a new file.

An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the **rollover** time, expressed in minutes.

The **retention** option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.

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

<b>Default</b>	rollover 1440 retention 12
<b>Parameters</b>	<i>minutes</i> — The rollover time, in minutes.
	<b>Values</b> 5 to 10080
	<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.
	<b>Default</b> 12
	<b>Values</b> 1 to 500

### 6.8.2.5 Event Filter Commands

#### filter

<b>Syntax</b>	[no] filter <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 to 1000

---

## default-action

<b>Syntax</b>	<b>default-action {drop   forward}</b> <b>no default-action</b>
<b>Context</b>	config>log>filter
<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>	default-action forward
<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>

## entry

<b>Syntax</b>	<b>[no] entry entry-id</b>
<b>Context</b>	config>log>filter
<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.

---

<b>Parameters</b>	<i>entry-id</i> — 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.
<b>Values</b>	1 to 999

## action

<b>Syntax</b>	<b>action {drop   forward}</b> <b>no action</b>
<b>Context</b>	config>log>filter filter-id>entry
<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 <a href="#">default-action</a> 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 <a href="#">action</a> statement.</p>
<b>Default</b>	Action specified by the <a href="#">default-action</a> command will apply.
<b>Parameters</b>	<b>drop</b> — Specifies packets matching the entry criteria will be dropped. <b>forward</b> — Specifies packets matching the entry criteria will be forwarded.

## match

<b>Syntax</b>	<b>[no] match</b>
<b>Context</b>	config>log>filter filter-id>entry
<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 <a href="#">application</a> 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</b> { <b>eq</b>   <b>neq</b> } <i>application-id</i> <b>no application</b>
<b>Context</b>	config>log>filter>entry>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 and so on. 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>	no application
<b>Parameters</b>	<b>eq</b>   <b>neq</b> — Specifies the operator match type. Valid operators are listed in <a href="#">Table 92</a> .

**Table 92 Valid Operators**

Operator	Notes
<b>eq</b>	equal to
<b>neq</b>	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, gsmp, 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</b> { <b>eq</b>   <b>neq</b> } <i>pattern pattern</i> [ <i>regexp</i> ] <b>no message</b>
<b>Context</b>	config>log>filter>entry>match
<b>Description</b>	<p>This command adds system messages as a match criterion.</p> <p>The <b>no</b> form of the command removes messages as a match criterion.</p>
<b>Parameters</b>	<b>eq</b> — Determines if the matching criteria should be equal to the specified value.

**neq** — Determines if the matching criteria should not be equal to the specified value.

*pattern* — Specifies a message up to 400 characters in length to be used in the match criteria.

**regexp** — Specifies the type of string comparison to use to determine if the log event matches the value of **message** command parameters. When the **regexp** keyword is not specified, the default matching algorithm used is a basic substring match.

## number

<b>Syntax</b>	<b>number</b> { <b>eq</b>   <b>neq</b>   <b>lt</b>   <b>lte</b>   <b>gt</b>   <b>gte</b> } <i>event-id</i> <b>no number</b>
<b>Context</b>	config>log>filter>entry>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>	no event-number
<b>Parameters</b>	<b>eq</b>   <b>neq</b>   <b>lt</b>   <b>lte</b>   <b>gt</b>   <b>gte</b> — Specifies the type of match. Valid operators are listed in <a href="#">Table 93</a> .

**Table 93 Valid Operators**

Operator	Notes
<b>eq</b>	equal to
<b>neq</b>	not equal to
<b>lt</b>	less than
<b>lte</b>	less than or equal to
<b>gt</b>	greater than
<b>gte</b>	greater than or equal to

*event-id* — The event ID, expressed as a decimal integer.

**Values** 1 to 4294967295

## router

- Syntax** **router** {**eq** | **neq**} *router-instance* [**regexp**]  
**no router**
- Context** config>log>filter>entry>match
- Description** This command specifies the log event matches for the router.
- Parameters** **eq** — Determines if the matching criteria should be equal to the specified value.  
**neq** — Determines if the matching criteria should not be equal to the specified value.  
*router-instance* — Specifies a router name up to 32 characters in length to be used in the match criteria.  
**regexp** — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** keyword is specified, the string in the **router** command is a regular expression string that will be matched against the subject string in the log event being filtered.

## severity

- Syntax** **severity** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *severity-level*  
**no severity**
- Context** config>log>filter>entry>match
- Description** This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command.  
  
The **no** form of the command removes the severity match criterion.
- Default** no severity
- Parameters** **eq** | **neq** | **lt** | **lte** | **gt** | **gte** — Specifies the match type. Valid operators are listed in [Table 94](#).

**Table 94** Valid Operators

Operator	Notes
<b>eq</b>	equal to
<b>neq</b>	not equal to
<b>lt</b>	less than
<b>lte</b>	less than or equal to

**Table 94** Valid Operators (Continued)

Operator	Notes
gt	greater than
gte	greater than or equal to

*severity-name* — Specifies the ITU severity level name. [Table 95](#) lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

**Table 95** ITU Severity Information

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>entry>match

**Description** This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

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

**Default** no subject

**Parameters** **eq** | **neq** — Specifies the match type. Valid operators are listed in [Table 96](#).



**Table 96 Valid Operators**

Operator	Notes
<b>eq</b>	equal to
<b>neg</b>	not equal to

*subject* — Specifies a string used as the subject match criterion.

**regex** — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regex** 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 **regex** keyword is not specified, the **subject** command string is matched exactly by the event filter.

## 6.8.2.6 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>	<p>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.</p> <p>The <b>no</b> form of the command removes the specified EHS handler action-list entry.</p>
<b>Parameters</b>	<i>entry-id</i> — Specifies the identifier of the EHS handler entry.
<b>Values</b>	1 to 1500

## min-delay

<b>Syntax</b>	<b>min-delay</b> [ <i>delay</i> ] <b>no min-delay</b>
<b>Context</b>	config>log>event-handling>handler>action-list>entry
<b>Description</b>	This command specifies the minimum delay in seconds between subsequent executions of the action specified in this entry. This is useful, for example, to ensure that a script doesn't get triggered to execute too often.
<b>Default</b>	no min-delay
<b>Parameters</b>	<i>delay</i> — Specifies the unit in seconds.
<b>Values</b>	1 to 604800

## 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>Default</b>	no script policy
<b>Parameters</b>	<p><i>policy-name</i> — Specifies the script policy name. Can be up to 32 characters maximum.</p> <p><b>owner</b> <i>policy-owner</i> — Specifies the script policy owner. Can be up to 32 characters maximum.</p> <p><b>Default</b> "TiMOS CLI"</p>

## 6.8.2.7 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>	[no] <b>event</b> <i>application-id 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>

---

*event-name-id* — Specifies the name or numerical identifier of the event.

**Values** 0 to 4294967295 | *event-name*: 32 characters max

## trigger-entry

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

**Context** config>log>event-trigger>event

**Description** 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.

The **no** form of the command removes the specified trigger entry.

**Parameters** *entry-id* — Specifies the identifier of the EHS event trigger entry.

**Values** 1 to 1500

## debounce

**Syntax** **debounce** *occurrences* [**within** *seconds*]  
**no debounce**

**Context** config>log>event-trigger>event>trigger-entry

**Description** This command configures when to trigger, for example after one or more event occurrences. The number of occurrences of an event can be bounded by a time window or left open.

**Default** no debounce

**Parameters** *occurrences* — specifies the number of times an event must occur for EHS to trigger a response

**Values** 2 to 15

**within** *seconds* — specifies the time window within which a specific event must occur a number of times equivalent to the specified *occurrences* for EHS to trigger a response

**Values** 1 to 604800

## event-handler

**Syntax** **event-handler** *event-handler*  
**no event-handler**

---

<b>Context</b>	config>log>event-trigger>event>trigger-entry
<b>Description</b>	This command configures the event handler to be used for this trigger entry.
<b>Parameters</b>	<i>event-handler</i> — Specifies the name of the event handler up to 32 characters in length.

## log-filter

<b>Syntax</b>	<b>log-filter</b> <i>filter-id</i> <b>no log-filter</b>
<b>Context</b>	config>log>event-trigger>event>trigger-entry
<b>Description</b>	<p>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.</p> <p>It is typically unnecessary to configure match criteria for the 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 <b>config&gt;log&gt;event-trigger</b></p>
<b>Parameters</b>	<p><i>filter-id</i> — Specifies the identifier of the filter.</p> <p><b>Values</b> 1 to 1500</p>

## 6.8.2.8 Log ID Commands

### log-id

<b>Syntax</b>	[no] <b>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 15 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>

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

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages. Log-ID 100 captures log messages with a severity level of major and above.



**Note:** Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.

The **no** form of the command deletes the log destination ID from the configuration.

Default	no log-id
Parameters	<i>log-id</i> — Specifies log ID number, expressed as a decimal integer.
Values	1 to 100

filter

Syntax	<b>filter</b> <i>filter-id</i> <b>no filter</b>
Context	config>log>log-id
Description	<p>This command adds an event filter policy with the log destination.</p> <p>The <b>filter</b> command is optional. If an event filter is not 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>
Default	no filter

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

**Values** 1 to 1000

## from

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

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

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

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

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

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

**Default** no from

**Parameters** **main** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the [filter](#) 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.

---

## python-policy

<b>Syntax</b>	<b>python-policy</b> <i>policy-name</i> <b>no python-policy</b>
<b>Context</b>	config>log>log-id
<b>Description</b>	<p>This command associates the Python script with the events sent to this log ID. The Python policy can be associated with the log only if the destination in the log ID is set <b>to syslog</b>.</p> <p>For information about Python policy configuration, refer to the Python Script Support for ESM in the <i>7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide</i>.</p> <p>The <b>no</b> form of this command disables Python processing of the events in this log ID.</p>
<b>Default</b>	no python-policy
<b>Parameters</b>	<i>policy-name</i> — Specifies a Python policy name up to 32 characters in length

## time-format

<b>Syntax</b>	<b>time-format</b> { <b>local</b>   <b>utc</b> }
<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>	time-format utc
<b>Parameters</b>	<b>local</b> — Specifies that timestamps are written in the system's local time. <b>utc</b> — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

## to cli

<b>Syntax</b>	<b>to cli</b> [ <i>size</i> ]
<b>Context</b>	config>log>log-id
<b>Description</b>	<p>This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs log events to be directed to CLI sessions. An operator can subscribe to a CLI log from within a CLI session using the <b>tools perform log subscribe-to log-id</b> command. The events are sent to the CLI session for the duration of that CLI session or until an <b>unsubscribe-from</b> command is issued.</p> <p>A local circular memory log is maintained for CLI logs.</p>



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 a log needs to be modified, the log ID must be removed and then re-created.

<b>Parameters</b>	<i>size</i> — Indicates the number of events that can be stored in the router's memory.
<b>Default</b>	100
<b>Values</b>	50 to 3000

## to console

<b>Syntax</b>	<b>to console</b>
<b>Context</b>	config>log>log-id
<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
<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> <p>When the <b>file-id</b> 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 <b>clear&gt;log</b> 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.</p>

---

<b>Default</b>	No destination is specified.
<b>Parameters</b>	<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 log-file-id</b> context.
<b>Values</b>	1 to 99

## to memory

<b>Syntax</b>	<b>to memory</b> [ <i>size</i> ]
<b>Context</b>	config>log>log-id
<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. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.</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>	to memory 100
<b>Parameters</b>	<i>size</i> — Indicates the number of events that can be stored in the memory.
<b>Values</b>	50 to 3000
<b>Default</b>	100

## to netconf

<b>Syntax</b>	<b>to netconf</b> [ <i>size</i> ]
<b>Context</b>	config>log>log-id
<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 NETCONF log or stream. A NETCONF log or stream can be subscribed to by one or more NETCONF sessions.</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>	to netconf 100
<b>Parameters</b>	<i>size</i> — Indicates the number of events that can be stored in the memory.
<b>Values</b>	50 to 3000
<b>Default</b>	100

## to session

<b>Syntax</b>	<b>to session</b>
<b>Context</b>	config>log>log-id
<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 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 <i>session</i> destination is saved in the configuration file but the “to session” part is not stored.</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

## to snmp

<b>Syntax</b>	<b>to snmp</b> [ <i>size</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. This command instructs the alarms and traps to be directed to the <b>snmp-trap-group</b> associated with <i>log-id</i>.</p> <p>A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the <i>log-id</i>.</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>	to snmp 100

---

<b>Parameters</b>	<i>size</i> — Specifies the number of events stored in this memory log.
<b>Values</b>	50 to 3000
<b>Default</b>	100

## 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 to 10</p>

## 6.8.2.9 SNMP Trap Groups

### snmp-trap-group

<b>Syntax</b>	[no] <b>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>

To suppress the generation of all alarms and traps see the [event-control](#) command. To suppress alarms and traps that are sent to this log-id, see the [filter](#) command. Once alarms and traps are generated they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.

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

<b>Default</b>	There are no default SNMP trap groups.
<b>Parameters</b>	<i>log-id</i> — Specifies the log ID value of a log configured in the <a href="#">log-id</a> context. Alarms and traps cannot be sent to the trap receivers until a valid <i>log-id</i> exists.
<b>Values</b>	1 to 99

## 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>	This command configures a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the [log-id](#), [snmp-trap-group](#) and at least one [trap-target](#) must be configured.

The [trap-target](#) command is used to add/remove a trap receiver from an [snmp-trap-group](#). The operational parameters specified in the command include:

- The IP address of the trap receiver
- The UDP port used to send the SNMP trap
- SNMP version
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

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

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

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



**Note:** 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.

*ip-address* — Specifies the IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group. *ipv6* applies to the 7750 SR only.

**Values**

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses

*port* — Specifies 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 to 65535

*snmpv1* | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the 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`

*community* | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If the **notify-community** is not configured, then no alarms or 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-name* — Specifies 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* — Specifies the *security-name* as defined in the **config>system>security>user** context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

**security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

**Default**      **no-auth-no-privacy**. This parameter can only be configured if SNMPv3 is also configured.

**Values**      `no-auth-no-privacy, auth-no-privacy, privacy`

**replay** — Enables the 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:** Due to 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 the **config>log>app-route-notifications** context can help reduce the probability of lost events.

## netconf-stream

<b>Syntax</b>	<b>netconf-stream</b> <i>stream-name</i> <b>no netconf-stream</b>
<b>Context</b>	config>log>log-id
<b>Description</b>	This command is used to associate a NETCONF stream name with a log ID. The NETCONF stream name must be unique per SR OS device. For the same log ID, <b>to netconf</b> must be configured for a subscription to that NETCONF stream name to be accepted. A <b>netconf-stream</b> cannot be set to "NETCONF" as "NETCONF" is reserved for log-id 101. If a <b>netconf-stream</b> is changed, active subscriptions to the changed stream name are terminated by SR OS.  The <b>no</b> form of this command removes a NETCONF stream name from a log ID. Active subscriptions to the removed stream name are terminated by SR OS.
<b>Default</b>	no netconf-stream
<b>Parameters</b>	<i>stream-name</i> — Specifies a NETCONF stream name up to 32 characters in length.

### 6.8.2.10 Syslog Commands

## syslog

<b>Syntax</b>	[no] <b>syslog</b> <i>syslog-id</i>
<b>Context</b>	config>log
<b>Description</b>	This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.  A valid <i>syslog-id</i> must have the target syslog host address configured.



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

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

The syslog ID configured in the **configure/service/vprn** 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 **config>log**.

<b>Parameters</b>	<i>syslog-id</i> — The syslog ID number for the syslog destination, expressed as a decimal integer.
<b>Values</b>	1 to 10

address

<b>Syntax</b>	<b>address</b> <i>ip-address</i> <b>no address</b>				
<b>Context</b>	config>log>syslog				
<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>	no address				
<b>Parameters</b>	<p><i>ip-address</i> — Specifies the IP address of the syslog target host in dotted decimal notation. An IPv6-address applies only to the 7750 SR.</p> <p><b>Values</b></p> <table><tr><td>ipv4-address</td><td>a.b.c.d</td></tr><tr><td>ipv6-address</td><td>x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses ipv6-address x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H</td></tr></table>	ipv4-address	a.b.c.d	ipv6-address	x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses ipv6-address x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H
ipv4-address	a.b.c.d				
ipv6-address	x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses ipv6-address x:x:x:x:x:x:x[-interface] x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H				

d: [0..255]D  
interface: 32 characters maximum, mandatory for link local addresses

facility

<b>Syntax</b>	<b>facility</b> <i>syslog-facility</i> <b>no facility</b>
<b>Context</b>	config>log>syslog
<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>	facility local7
<b>Parameters</b>	<p><i>syslog-facility</i> — Specifies a syslog facility name which represents a specific numeric facility code. The code must 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> <p>Valid responses per RFC3164, <i>The BSD syslog Protocol</i>, are listed in <a href="#">Table 97</a>.</p>

**Table 97 Syslog Protocol Valid Responses**

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
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

**Values** 0 to 23

## level

- Syntax** **level** *syslog-level*  
**no level**
- Context** config>log>syslog
- Description** This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.
- Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.
- The **no** form of the command reverts to the default value.
- Default** level info
- Parameters** *value* — Specifies the threshold severity level name.
- Values** emergency, alert, critical, error, warning, notice, info, debug

**Table 98** Level Parameter Value Descriptions

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

## log-prefix

- Syntax** **log-prefix** *log-prefix-string*  
**no log-prefix**
- Context** config>log>syslog

---

<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 an alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.</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 to 9) characters.</p> <p>The <b>no</b> form of the command removes the log prefix string.</p>
<b>Default</b>	no log-prefix
<b>Parameters</b>	<p><i>log-prefix-string</i> — Specifies an alphanumeric string up to 32 characters in length. Spaces and colons ( : ) cannot be used in the string.</p>

## port

<b>Syntax</b>	<p><b>port</b> <i>value</i></p> <p><b>no port</b></p>
<b>Context</b>	config>log>syslog
<b>Description</b>	<p>This command configures the UDP port that will be used to send syslog messages to the syslog target host.</p> <p>The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.</p> <p>Only one port can be configured. If multiple <b>port</b> commands are entered, the last entered port overwrites the previously entered ports.</p> <p>The <b>no</b> form of the command reverts to default value.</p>
<b>Default</b>	no port
<b>Parameters</b>	<p><i>value</i> — Specifies the value that is the configured UDP port number used when sending syslog messages.</p> <p><b>Values</b>      1 to 65535</p>



## 6.9 Log Command Reference

### 6.9.1 Command Hierarchies

- [Show Commands](#)
- [Clear Command](#)
- [Tools Commands](#)

#### 6.9.1.1 Show Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* for information about log show routines for VPRN services.

```
show
  — log
    — accounting-policy [acct-policy-id] [access | network] [associations]
    — accounting-records
    — applications
    — event-control [application-id [event-name | event-number]]
    — event-control application-id event-name detail
    — event-handling
      — handler [handler-name]
      — handler detail
      — information
      — scripts
    — event-parameters [application-id [event-name | event-number]]
    — file-id [log-file-id]
    — filter-id [filter-id]
    — log-collector
    — log-id [log-id] [severity severity-level] [application application] [sequence from-seq
      [to-seq]] [count count] [router router-instance [expression] [subject subject
      [regex]]] [ascending | descending] [message format [msg-regex]]
    — snmp-trap-group [log-id]
    — syslog [syslog-id]
```

#### 6.9.1.2 Clear Command

```
clear
  — log log-id
  — log
    — log-id log-id
    — event-handling
```

- **handler** *event-handler-name*
- **information**

### 6.9.1.3 Tools Commands

```
tools
  — dump
    — log
      — all-subscriptions
      — subscriptions
  — perform
    — log
      — subscribe-to log-id log-id
      — unsubscribe-from log-id log-id
```

## 6.9.2 Command Descriptions

- [Show Commands](#)
- [Clear Commands](#)
- [Tools Commands](#)

### 6.9.2.1 Show Commands

The command output in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### accounting-policy

<b>Syntax</b>	accounting-policy [ <i>acct-policy-id</i> ] [ <b>access</b>   <b>network</b> ] [ <b>associations</b> ]
<b>Context</b>	show>log
<b>Description</b>	This command displays accounting policy information.
<b>Parameters</b>	<i>policy-id</i> — Specifies the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.
<b>Values</b>	1 to 99
	<b>access</b> — Specifies to only display access accounting policies.
	<b>network</b> — Specifies to only display network accounting policies.



**association** — Displays accounting-policy associations

**Output** The following is an example of accounting policy information.

Table 99 describes accounting policy output fields.

### Sample Output

```
A:ALA-1# show log accounting-policy
=====
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
10     access  Yes  Up    Up    5      3      complete-service-ingress-egress
=====

A:ALA-1#

A:ALA-1# show log accounting-policy 10
=====
Accounting Policies
=====
Policy Type      Def Admin Oper  Intvl      File Record Name
Id              State State
-----
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 Id	Type	Def State	Admin State	Oper State	Intvl	File Id	Record Name
-----------	------	-----------	-------------	------------	-------	---------	-------------

-----

10	access	Yes	Up	Up	5	3	complete-service-ingress
----	--------	-----	----	----	---	---	--------------------------

=====

A:ALA-1#

**Table 99 Show Accounting Policy Output Fields**

Label	Description
Policy ID	The identifying value assigned to a specific policy.
Type	Identifies accounting record type forwarded to the configured accounting file. access — Indicates that the policy is an access accounting policy. network — Indicates that the policy is a network accounting policy. none — Indicates no accounting record types assigned.
Def	Yes — Indicates that the policy is a default access or network policy. No — Indicates that the policy is not a default access or network policy.
Admin State	Displays the administrative state of the policy. Up — Indicates that the policy is administratively enabled. Down — Indicates that the policy is administratively disabled.
Oper State	Displays the operational state of the policy. Up — Indicates that the policy is operationally up. Down — Indicates that the policy is operationally down.
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.

**Table 99 Show Accounting Policy Output Fields (Continued)**

Label	Description
This policy is applied to	Specifies the entity where the accounting policy is applied.

## accounting-records

- Syntax** accounting-records
- Context** show>log
- Description** This command displays accounting policy record names.
- Output** Accounting Records Output

Table 100 describes accounting records output fields.

**Table 100 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
=====
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>	The following is an example of log application information.

### Sample Output

```

*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-id* [*event-name* | *event-number*]]  
**event-control** *application-id* *event-name* **detail**

**Context** show>log

**Description** This command displays event control settings for events including whether the event is suppressed or generated and the severity level for the event.

If no options are specified all events, alarms and traps are listed.

**Parameters** **application-id** — Only displays event control for the specified application.

**Default** All applications.

The following are some sample applications:

**Values**

application\_assurance|aps|atm|auto\_prov|bfd|bgp|bier|  
bmp|calltrace|ccag|cflowd|chassis|cpmhwfilter|  
cpmhwqueue|debug|dhcp|dhcps|diameter|dot1x|dynsvc|  
efm\_oam|elmi|ering|eth\_cfm|etun|filter|fpe|gsmpp|gmpls|  
gtp|gtungrp|icl|igh|igmp|igmp\_snooping|ip|ipfix|ipsec|  
ipsec\_cpm|isis|l2tp|lag|ldap|ldp|li|lldp|lmp|logger|  
macsec|mcac|mcpaht|mc\_redundancy|mgmt\_core|mirror|mld|  
mld\_snooping|mpls|mpls\_tp|mpls\_lmgr|mrp|msdp|nat|nge|  
ntp|oam|open\_flow|ospf|pcap|pcep|pfcp|pim|  
pim\_snooping|port|ppp|pppoe|pppoe\_clnt|profile|ptp|  
pxc|python|qos|radius|rib\_api|rip|rip\_ng|  
route\_next\_hop|route\_policy|rpki|rsvp|security|sflow|  
snmp|sr\_policy|stp|subscr\_mgmt|sub\_host\_trk|svcmgr|  
system|tip|tls|user|user\_db|video|vrrp|vrtr|wlan\_gw|wpp

**event-name** — Only displays event control for the named application event, up to 32 characters.

**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** The following is an example of event control information.

[Table 101](#) describes the output fields for the event control.

**Table 101 Event-Control Output Field Descriptions**

Label	Description
Application	The application name.
ID#	The event ID number within the application. L ID# An “L” in front of an ID represents event types that do not generate an associated SNMP notification. Most events do generate a notification, only the exceptions are marked with a preceding “L”.
Event Name	The event name.
P	CL — The event has a cleared severity or priority. CR — The event has critical severity or priority. IN — The event has indeterminate severity or priority. MA — The event has major severity or priority. MI — The event has minor severity or priority. WA — The event has warning severity or priority.
g/s	gen — The event will be generated or logged by event control. sup — The event will be suppressed or dropped by event control. thr — Specifies that throttling is enabled.
Logged	The number of events logged or generated.
Dropped	The number of events dropped/suppressed.
Severity	The severity level of the event (cleared, indeterminate, critical, major, minor, or warning).
Generated	Indicates whether the log event is enabled (true) or suppressed (false).
Count	The number of events logged or generated.
Drop count	The number of events dropped/suppressed.
Throttle	Indicates whether the event is subject to global throttling (true or false).
Specific throttle	Indicates whether the event is subject to specific per event throttling (true or false).
Specific throttle limit	The configured number of events per interval for specific throttling.
Specific throttle interval (s)	The configured interval over which the specific throttling limit is applied.

**Table 101 Event-Control Output Field Descriptions (Continued)**

Label	Description (Continued)
Specific throttle by default	Indicates whether the specific throttling is enabled or not when it has not been explicitly configured.
Specific throttle limit default	The default number of events per-interval for specific throttling of this event.
Specific throttle interval default (s)	The default interval over which the specific default throttling limit is applied.
Repeat	Specifies that the log event should be repeated every minute until the underlying condition is cleared.

### Sample Output

The following is a sample output:

```
A:gal171# show log event-control
=====
Log Events
=====
Application
ID#      Event Name                                P   g/s      Logged      Dropped
-----
BGP:
  2001  bgpEstablished                          MI  gen        0           0
  2002  bgpBackwardTransition                     WA  gen        0           0
  2003  tBgpMaxPrefix90                            WA  gen        0           0
  2004  tBgpMaxPrefix100                           CR  gen        0           0
L  2005  sendNotification                          WA  gen        0           0
L  2006  receiveNotification                       WA  gen        0           0
L  2007  bgpInterfaceDown                          WA  gen        0           0
L  2008  bgpConnNoKA                              WA  gen        0           0
L  2009  bgpConnNoOpenRcvd                         WA  gen        0           0
L  2010  bgpRejectConnBadLocAddr                   WA  gen        0           0
L  2011  bgpRemoteEndClosedConn                    WA  gen        0           0
L  2012  bgpPeerNotFound                          WA  gen        0           0
L  2013  bgpConnMgrTerminated                      WA  gen        0           0
L  2014  bgpTerminated                            WA  gen        0           0
L  2015  bgpNoMemoryPeer                          CR  gen        0           0
L  2016  bgpVariableRangeViolation                 WA  gen        0           0
L  2017  bgpCfgViol                              WA  gen        0           0
CFLOWD:
  2001  cflowdCreated                          MI  gen        0           0
  2002  cflowdCreateFailure                      MA  gen        0           0
  2003  cflowdDeleted                          MI  gen        0           0
  2004  cflowdStateChanged                      MI  gen        0           0
  2005  cflowdCleared                          MI  gen        0           0
  2006  cflowdFlowCreateFailure                 MI  gen        0           0
  2007  cflowdFlowFlushFailure                  MI  gen        0           0
  2008  cflowdFlowUnsuppProto                   MI  sup        0           0
CCAG:
CHASSIS:
  2001  cardFailure                          MA  gen        0           0
```

---

2002	cardInserted	MI	gen	4	0
2003	cardRemoved	MI	gen	0	0
2004	cardWrong	MI	gen	0	0
2005	EnvTemperatureTooHigh	MA	gen	0	0
...					
DEBUG:					
L 2001	traceEvent	MI	gen	0	0
DOT1X:					
FILTER:					
2001	filterPBRPacketsDropped	MI	gen	0	0
IGMP:					
2001	vRtrIgmpIfRxQueryVerMismatch	WA	gen	0	0
2002	vRtrIgmpIfCModeRxQueryMismatch	WA	gen	0	0
IGMP_SNOOPING:					
IP:					
L 2001	clearRTMError	MI	gen	0	0
L 2002	ipEtherBroadcast	MI	gen	0	0
L 2003	ipDuplicateAddress	MI	gen	0	0
L 2004	ipArpInfoOverwritten	MI	gen	0	0
L 2005	fibAddFailed	MA	gen	0	0
L 2006	qosNetworkPolicyMallocFailed	MA	gen	0	0
L 2007	ipArpBadInterface	MI	gen	0	0
L 2008	ipArpDuplicateIpAddress	MI	gen	0	0
L 2009	ipArpDuplicateMacAddress	MI	gen	0	0
ISIS:					
2001	vRtrIsisDatabaseOverload	WA	gen	0	0
2002	vRtrIsisManualAddressDrops	WA	gen	0	0
2003	vRtrIsisCorruptedLSPDetected	WA	gen	0	0
2004	vRtrIsisMaxSeqExceedAttempt	WA	gen	0	0
2005	vRtrIsisIDLenMismatch	WA	gen	0	0
2006	vRtrIsisMaxAreaAdrsMismatch	WA	gen	0	0
....					
USER:					
L 2001	cli_user_login	MI	gen	2	0
L 2002	cli_user_logout	MI	gen	1	0
L 2003	cli_user_login_failed	MI	gen	0	0
L 2004	cli_user_login_max_attempts	MI	gen	0	0
L 2005	ftp_user_login	MI	gen	0	0
L 2006	ftp_user_logout	MI	gen	0	0
L 2007	ftp_user_login_failed	MI	gen	0	0
L 2008	ftp_user_login_max_attempts	MI	gen	0	0
L 2009	cli_user_io	MI	sup	0	48
L 2010	snmp_user_set	MI	sup	0	0
L 2011	cli_config_io	MI	gen	4357	0
VRRP:					
2001	vrrpTrapNewMaster	MI	gen	0	0
2002	vrrpTrapAuthFailure	MI	gen	0	0
2003	tmnxVrrpIPListMismatch	MI	gen	0	0
2004	tmnxVrrpIPListMismatchClear	MI	gen	0	0
2005	tmnxVrrpMultipleOwners	MI	gen	0	0
2006	tmnxVrrpBecameBackup	MI	gen	0	0
L 2007	vrrpPacketDiscarded	MI	gen	0	0
VRTR:					
2001	tmnxVRtrMidRouteTCA	MI	gen	0	0
2002	tmnxVRtrHighRouteTCA	MI	gen	0	0
2003	tmnxVRtrHighRouteCleared	MI	gen	0	0
2004	tmnxVRtrIllegalLabelTCA	MA	gen	0	0
2005	tmnxVRtrMcastMidRouteTCA	MI	gen	0	0



```

2006 tmnxVRtrMcastMaxRoutesTCA      MI  gen      0      0
2007 tmnxVRtrMcastMaxRoutesCleared  MI  gen      0      0
2008 tmnxVRtrMaxArpEntriesTCA       MA  gen      0      0
2009 tmnxVRtrMaxArpEntriesCleared   MI  gen      0      0
2011 tmnxVRtrMaxRoutes               MI  gen      0      0
=====

```

A:ALA-1#

A:ALA-1# show log event-control ospf

Log Events

Application

ID#	Event Name	P	g/s	Logged	Dropped
2001	ospfVirtIfStateChange	WA	gen	0	0
2002	ospfNbrStateChange	WA	gen	1	0
2003	ospfVirtNbrStateChange	WA	gen	0	0
2004	ospfIfConfigError	WA	gen	0	0
2005	ospfVirtIfConfigError	WA	gen	0	0
2006	ospfIfAuthFailure	WA	gen	0	0
2007	ospfVirtIfAuthFailure	WA	gen	0	0
2008	ospfIfRxBadPacket	WA	gen	0	0
2009	ospfVirtIfRxBadPacket	WA	gen	0	0
2010	ospfTxRetransmit	WA	sup	0	0
2011	ospfVirtIfTxRetransmit	WA	sup	0	0
2012	ospfOriginateLsa	WA	sup	0	404
2013	ospfMaxAgeLsa	WA	gen	3	0
2014	ospfLsdbOverflow	WA	gen	0	0
2015	ospfLsdbApproachingOverflow	WA	gen	0	0
2016	ospfIfStateChange	WA	gen	2	0
2017	ospfNssaTranslatorStatusChange	WA	gen	0	0
2018	vRtrOspfSpfRunsStopped	WA	gen	0	0
2019	vRtrOspfSpfRunsRestarted	WA	gen	0	0
2020	vRtrOspfOverloadEntered	WA	gen	1	0
2021	vRtrOspfOverloadExited	WA	gen	0	0
2022	ospfRestartStatusChange	WA	gen	0	0
2023	ospfNbrRestartHelperStatusChange	WA	gen	0	0
2024	ospfVirtNbrRestartHelperStsChg	WA	gen	0	0

A:ALA-1#

A:ALA-1# show log event-control ospf ospfVirtIfStateChange

Log Events

Application

ID#	Event Name	P	g/s	Logged	Dropped
2001	ospfVirtIfStateChange	WA	gen	0	0

A:ALA-1#

A:dut-c# show log event-control "BGP" tBgpMaxNgPfxLmtThresholdReached detail

Log event "tBgpMaxNgPfxLmtThresholdReached"

Severity : major

```
Generated : true
Count : 0
Drop count : 1
Throttle : false
Specific throttle : false
Specific throttle limit : 0
Specific throttle interval (s) : 0
Specific throttle by default : false
Specific throttle limit default : 0
Specific throttle interval default(s) : 0
Repeat : false

# show log event-control "mgmt_core"
=====
Log Events
=====
Application
ID#      Event Name                P   g/s      Logged      Dropped
-----
L  2001 mdConfigChange            MI  sup          0        1339
=====
```

event-handling

- Syntax** event-handling
- Context** show>log
- Description** This command enables the context to display Event Handling System (EHS) information.

handler

- Syntax** handler [handler-name]  
handler detail
- Context** show>log>event-handling
- Description** This command enters the context to display EHS handler information.
- Parameters** handler-name — Specifies the name of a specific handler up to 32 characters in length.  
detail — Keyword to list details of all handlers.
- Output** The following is an example of handler information.  
[Table 102](#) describes handler output fields.

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
=====

```

**Table 102**     **Handler Output Field Descriptions**

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.
<b>Handler Action-List Entry</b>	
Entry-id	The action-list entry identifier.
Description	The action-list entry description string.
Admin State	The administrative state of the action-list entry.

Table 102     Handler Output Field Descriptions (Continued)

Label	Description (Continued)
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.

information

- Syntax

information
- Context

show>log>event-handling
- Description

This command displays general information about EHS, as well as handler and trigger statistics.
- Output

Show Information Output

Sample output

```
=====
Event Handling System - Event Trigger Statistics
=====

Application Name
Event Id                Total      Success  ErrNoEntry  AdmStatus
-----
```

OAM								
2001			0	0	0	0		
-----								
Entry	FilMatch	Trigger	Debounce	FilFail	ErrAdmSta	ErrFilter	ErrHandler	
-----								
1	0	0	0	0	0	0	0	
10	0	0	0	0	0	0	0	
-----								
SUM	0	0	0	0	0	0	0	
=====								
Application Name								
Event Id			Total	Success	ErrNoEntry	AdmStatus		
-----								
OAM								
2004			0	0	0	0		
-----								
Entry	FilMatch	Trigger	Debounce	FilFail	ErrAdmSta	ErrFilter	ErrHandler	
-----								
1	0	0	0	0	0	0	0	
-----								
SUM	0	0	0	0	0	0	0	
=====								
EVENTS PROCESSED			Total	Success	ErrNoEntry	AdmStatus		
-----								
			0	0	0	0		
=====								
-----								
Event Handling System - Event Handler Statistics								
=====								
-----								
Handler			Total	Success	ErrNoEntry	AdmStatus		
my-handler-1			0	0	0	0		
-----								
Entry	Id	Launch	MinDelay	ErrLaunch	ErrAdmSta			
-----								
1		0	0	0	0			
-----								
SUMMARY		0	0	0	0			
=====								
HANDLERS SUMMARY			Total	Success	ErrNoEntry	AdmStatus		
-----								
			0	0	0	0		
=====								

scripts

Syntax	scripts
Context	show>log>event-handling
Description	This command displays handler configuration and script run queue information.
Output	Show Scripts Output

Sample output

```
=====
Event Handling System - Script Policy Association
=====
-----
No Matching Entries Found
=====
Event Handling System - Script Association
=====
-----
No Matching Entries Found
=====
Event Handling System - Script Launched List
=====
Run #      Script owner      Script name      Script state
-----
No Matching Entries
=====
```

event-parameters

<b>Syntax</b>	<b>event-parameters</b> [ <i>application-id</i> [ <i>event-name</i>   <i>event-number</i> ]]
<b>Context</b>	show>log
<b>Description</b>	This command displays an event's (or all events) common parameters and specific parameters. This allows a user to know what parameters can be passed from a triggering event to the triggered EHS script.
<b>Parameters</b>	<p><i>application-id</i> — Displays event parameters for the specified application.</p> <p><b>Default</b> All applications.</p> <p>The following are some sample applications:</p> <p><b>Values</b> application_assurance, aps, atm, bfd, bgp, calltrace, ccag, cflowd, chassis, cpmhwfilter, cpmhwqueue, debug, dhcp, dhcps, diameter, dot1x, dynsvc, efm_oam, elmi, ering, eth_cfm, etun, filter, fpe, gsmp, gmpls, gtungrp, icl, igh, igmp, igmp_snooping, ip, ipfix, ipsec, ipsec_cpm, isis, l2tp, lag, ldap, ldp, li, lldp, lmp, logger, mcac, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, mpls_tp, mrp, msdp, nat, ntp, oam, open_flow, ospf, pcep, pim, pim_snooping, port, ppp, pppoe, ptp, pxc, python, qos, radius, rip, rip_ng, route_next_hop, route_policy, rpki, rsvp, security, sflow, snmp, stp, subscr_mgmt, sub_host_trk, svcmgr, system, tip, tls, user, user_db, video, vrrp, vrtr, wlan_gw, wpp</p> <p><i>event-name</i> — Displays event parameters for the named application event up to 32 characters in length.</p> <p><b>Default</b> All events for the application.</p>

*event-number* — Displays event parameters for the specified application event number.

<b>Default</b>	All events for the application.
----------------	---------------------------------

**Values** 0 — 4294967295

**Output** The following displays log event parameter information.

## Sample output

```
# show log event-parameters "oam" 2001
=====
Common Event Parameters
    appid
    name
    eventid
    severity
    subject
    gentime
Event Specific Parameters
    tmnxOamPingCtlOwnerIndex
    tmnxOamPingCtlTestIndex
    tmnxOamPingCtlTgtAddrType
    tmnxOamPingCtlTgtAddress
    tmnxOamPingResultsTestRunIndex
    tmnxOamPingResultsOperStatus
    tmnxOamPingResultsMinRtt
    tmnxOamPingResultsMaxRtt
    tmnxOamPingResultsAverageRtt
    tmnxOamPingResultsRttSumOfSquares
    tmnxOamPingResultsRttOfSumSquares
    tmnxOamPingResultsMtuResponseSize
    tmnxOamPingResultsSvcPing
    tmnxOamPingResultsProbeResponses
    tmnxOamPingResultsSentProbes
    tmnxOamPingResultsLastGoodProbe
    tmnxOamPingCtlTestMode
    tmnxOamPingHistoryIndex
=====
```

## file-id

**Syntax**     **file-id** [*log-file-id*]

**Context** show>log

**Description** This command displays event file log information.

If no command line parameters are specified, a summary output of all event log files is displayed.

Specifying a file ID displays detailed information on the event file log.

**Parameters** *log-file-id* — Displays detailed information on the specified event file log.

**Output**    The following shows log file summary information.

[Table 103](#) describes the output fields for a log file summary.

**Table 103    Log File Summary Output Fields**

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

- Syntax** filter-id [*filter-id*]
- Context** show>log
- Description** This command displays event log filter policy information.
- Parameters** *filter-id* — Displays detailed information on the specified event filter policy ID.
- Values** 1 — 65535
- Output** The following displays event filter log information.

[Table 104](#) describes the output fields for event log filter summary information.

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#
```

**Sample Output**

```
*A:ALA-48>config>log# show log filter-id 1001
=====
Log Filter
=====
Filter-id      : 1001      Applied      : yes      Default Action: drop
Description    : Collect events for Serious Errors Log
-----
Log Filter Match Criteria
-----
Entry-id      : 10              Action      : forward
Application    :                  Operator     : off
Event Number   : 0              Operator     : off
Severity       : major          Operator     : greaterThanOrEqual
Subject        :                  Operator     : off
Match Type     : exact string              :
Router         :                  Operator     : off
Match Type     : exact string              :
Description    : Collect only events of major severity or higher
-----
=====
*A:ALA-48>config>log#
```

**Table 104**      **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.

Event Log Filter Detailed Output

[Table 105](#) describes the output fields for detailed event log filter information.

**Table 105 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 106](#) describes the output fields for log filter match criteria information.

**Table 106 Log Filter Match Criteria Output Fields**

Label	Description
Entry-id	The event log filter entry ID.
Action	default — There is no explicit action for the event log filter entry and the filter's default action is used on matching events. drop — The action for the event log filter entry is to drop matching events. forward — The action for the event log filter entry is to forward matching events.
Description (Entry-id)	The description string for the event log filter entry.
Application	The event log filter entry application match criterion.
Event Number	The event log filter entry application event ID match criterion.

**Table 106 Log Filter Match Criteria Output Fields (Continued)**

Label	Description
Severity	<p>cleared — The log event filter entry application event severity cleared match criterion.</p> <p>indeterminate — The log event filter entry application event severity indeterminate match criterion.</p> <p>critical — The log event filter entry application event severity critical match criterion.</p> <p>major — The log event filter entry application event severity cleared match criterion.</p> <p>minor — The log event filter entry application event severity minor match criterion.</p> <p>warning — 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>equal — Matches when equal to the match criterion.</p> <p>greaterThan — Matches when greater than the match criterion.</p> <p>greaterThanOrEqual — Matches when greater than or equal to the match criterion.</p> <p>lessThan — Matches when less than the match criterion.</p> <p>lessThanOrEqual — Matches when less than or equal to the match criterion.</p> <p>notEqual — Matches when not equal to the match criterion.</p> <p>off — No operator specified for the match criterion.</p>

## 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.
<b>Output</b>	<p>The following displays log collector information.</p> <p><a href="#">Table 107</a> describes log-collector output fields.</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#
```

**Table 107** Show Log-Collector Output Fields

Label	Description
<Collector Name>	<p>Main — The main event stream contains the events that are not explicitly directed to any other event stream.</p> <p>Security — The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted.</p> <p>Change — The change event stream contains all events that directly affect the configuration or operation of this node.</p> <p>Debug — 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>Enabled — Logging is enabled.</p> <p>Disabled — Logging is disabled.</p>

**Table 107 Show Log-Collector Output Fields (Continued)**

Label	Description
Dest. Type	<p>Console — 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>Session — 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>Syslog — Log events are sent to a syslog receiver.</p> <p>SNMP traps — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables.</p> <p>File — All selected log events will be directed to a file on one of the compact flash disks.</p> <p>Memory — All selected log events will be directed to an in-memory storage area.</p>

## log-id

**Syntax** **log-id** [*log-id*] [**severity** *severity-level*] [**application** *application*] [**sequence** *from-seq* [*to-seq*]] [**count** *count*] [**router** *router-instance* [**expression**]] [**message** *message* [**regular-expression**]] [**subject** *subject* [regexp]] [**ascending** | **descending**] [**message format** [msg-regexp]]

**Context** show>log

**Description** This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.

If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.

If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.

Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.

---

<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 to 99</p> <p><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> <p><i>application</i> — Displays only events generated by the specified application.</p> <p><b>Default</b> All applications</p> <p>The following values are examples of applications:</p> <p><b>Values</b> bgp, cflowd, chassis, dhcp, debug, filter, igmp, ip, isis, lag, ldp, lldp, logger, mirror, mpls, oam, ospf, pim, port, ppp, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr, ospf_ng, ntp</p> <p><b>expression</b> — Specifies to use a regular expression as match criteria for the router instance string.</p> <p><i>from-seq</i> [<i>to-seq</i>] — Displays the log entry numbers from a particular entry sequence number (<i>from-seq</i>) to another sequence number (<i>to-seq</i>). The <i>to-seq</i> value must be larger than the <i>from-seq</i> value.</p> <p>If the <i>to-seq</i> number is not provided, the log contents to the end of the log is displayed unless the <b>count</b> parameter is present in which case the number of entries displayed is limited by the <b>count</b>.</p> <p><b>Default</b> All sequence numbers</p> <p><b>Values</b> 1 to 4294967295</p> <p><i>count</i> — Limits the number of log entries displayed to the <i>number</i> specified.</p> <p><b>Default</b> All log entries</p> <p><b>Values</b> 1 to 4294967295</p> <p><i>router-instance</i> — Specifies a router name up to 32 characters in length to be used in the display criteria.</p> <p><i>format</i> — Specifies a message string up to 400 characters in length to be used in the display criteria.</p> <p><b>msg-regex</b> — Specifies to use a regular expression as parameters with the specified <i>message</i> string.</p> <p><i>subject</i> — Displays only log entries matching the specified text <i>subject</i> 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.</p> <p><b>regex</b> — Specifies to use a regular expression as parameters with the specified <i>subject</i> string.</p>
-------------------	---

**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** The following displays log ID information.

[Table 108](#) describes the log ID field output.

### Sample Output

```
A:bkvm30# show log log-id
=====
Event Logs
=====
```

Log Id	Source	Filter Id	Admin State	Oper State	Logged	Dropped	Dest Type	Dest Id	Size
1	none	none	up	down	0	0	none		N/A
5	D	none	up	up	0	0	cli		1024
15	M	none	up	up	24	0	cli		512
20	S	none	up	up	12	0	memory		256
21	C	none	up	up	258	0	memory		256
22	M S C	none	up	up	288	0	file	15	N/A
33	M S C	none	up	down	0	0	none		N/A
34	none	none	up	down	0	0	file	33	N/A
35	M S	none	up	up	36	0	memory		100
55	C	none	up	down	0	0	cli		500
77	S	none	up	up	0	0	cli		100
82	none	none	up	down	0	0	none		N/A
99	M	none	up	up	122	0	memory		500
100	M	1001	up	up	10	112	memory		500

```
=====
```

### Sample Memory or File Event Log Contents Output

```
A:admin@Dut-A# show log log-id log-id 10
=====
Event Log 10
=====
Description : (Not Specified)
Memory Log contents [size=100 next event=13 (not wrapped)]
12 2018/02/20 10:12:00.429 UTC MINOR: DEBUG #2001 Base GRPC
"GRPC: RPC-2: gNMI.Subscribe
Client URI: ipv4:192.99.5.0:49648
Username: admin
Received message of type gnmi.SubscribeRequest:
.request = subscribe:
.encoding: 0 = JSON
.mode: 0 = STREAM
.prefix: /
.subscription (1):
.path: /state/router[router-instance=*]/interface[interface-name=*]/ipv4/oper-
state
```



```
.mode: 1 = ON_CHANGE
.sample_interval: 10000000000
"
11 2018/02/20 10:12:00.422 UTC MINOR: DEBUG #2001 Base GRPC
"GRPC: RPC-2: gNMI.Subscribe
  Client URI: ipv4:192.99.5.0:49648
  Username: admin
  Client called RPC.
  Now waiting till first message arrive.
"

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#
```

**Table 108 Log-Id Output Field Descriptions**

Label	Description
Log Id	An event log destination.
Source	no — The event log filter is not currently in use by a log ID. yes — The event log filter is currently in use by a log ID.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Admin State	Up — Indicates that the administrative state is up. Down — Indicates that the administrative state is down.
Oper State	Up — Indicates that the operational state is up. Down — Indicates that the operational state is down.
Logged	The number of events that have been sent to the log source(s) that were forwarded to the log destination.
Dropped	The number of events that have been sent to the log source(s) that were not forwarded to the log destination because they were filtered out by the log filter.
Dest. Type	Console — All selected log events are directed to the system console. If the console is not connected, then all entries are dropped. Syslog — All selected log events are sent to the syslog address. SNMP traps — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables. File — All selected log events will be directed to a file on one of the CPM's compact flash disks. Memory — All selected log events will be directed to an in-memory storage area.
Dest ID	The event log stream destination.
Size	The allocated memory size for the log.
Time format	The time format specifies the type of timestamp format for events sent to logs where log ID destination is either syslog or file. When the time format is UTC, timestamps are written using the Coordinated Universal Time value. When the time format is local, timestamps are written in the system's local time.

## snmp-trap-group

<b>Syntax</b>	<b>snmp-trap-group</b> [ <i>log-id</i> ]
<b>Context</b>	show>log
<b>Description</b>	This command displays SNMP trap group configuration information.
<b>Parameters</b>	<i>log-id</i> — Displays only SNMP trap group information for the specified trap group log ID.
<b>Values</b>	1 to 99
<b>Output</b>	The following displays SNMP trap group information.

[Table 109](#) describes SNMP trap group output fields.

### Sample Output

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44
=====
SNMP Trap Group 44
=====
Description : none
-----
Name       : ntt-test
Address    : 10.10.10.3
Port      : 162
Version   : v2c
Community : ntttesting
Sec. Level : none
Replay    : disabled
Replay from : n/a
Last replay : never
-----
Name       : test2
Address    : 10.20.20.5
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#
```

**Table 109**      **SNMP Trap Group Output Fields**

Label	Description
Log-ID	The log destination ID for an event stream.
Address	The IP address of the trap receiver,

**Table 109** SNMP Trap Group Output Fields (Continued)

Label	Description
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are <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.

## 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 to 10

**Output** The following displays syslog information.

[Table 110](#) describes the syslog output fields.

### Sample Output

```
*A:ALA-48>config>log# show log syslog
=====
Syslog Target Hosts
=====
Id      Ip Address                                     Port      Sev Level
```

```

                Below Level Drop                Facility      Pfx Level
-----
2      unknown                514      info
      0                local7      yes
3      unknown                514      info
      0                local7      yes
5      unknown                514      info
      0                local7      yes
10     unknown                514      info
      0                local7      yes
=====
*A:ALA-48>config>log#

*A:MV-SR>config>log# show log syslog 1
=====
Syslog Target 1
=====
IP Address      : 192.168.15.22
Port            : 514
Log-ids         : none
Prefix          : Sr12
Facility        : local1
Severity Level  : info
Prefix Level    : yes
Below Level Drop : 0
Description     : Linux Station Springsteen
=====
*A:MV-SR>config>log#

```

**Table 110**      **Show Log Syslog Output Fields**

Label	Description
Syslog ID	The syslog ID number for the syslog destination.
IP Address	The IP address of the syslog target host.
Port	The configured UDP port number used when sending syslog messages.
Facility	The facility code for messages sent to the syslog target host.
Severity Level	The syslog message severity level threshold.
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.
Prefix Present	Yes — A log prefix was prepended to the syslog message sent to the syslog host. No — A log prefix was not prepended to the syslog message sent to the syslog host.
Description	A text description stored in the configuration file for a configuration context.

**Table 110 Show Log Syslog Output Fields (Continued)**

Label	Description
LogPrefix	The prefix string prepended to the syslog message.
Log-id	Events are directed to this <i>destination</i> .

## 6.9.2.2 Clear Commands

### log

<b>Syntax</b>	<b>log</b> <i>log-id</i>
<b>Context</b>	clear
<b>Description</b>	The <b>clear log</b> <i>log-id</i> command has been deprecated and replaced by the <b>clear log log-id</b> <i>log-id</i> command. The <b>clear log</b> <i>log-id</i> command continues to be supported, but it is recommended to use the <b>clear log log-id</b> <i>log-id</i> command instead.
<b>Parameters</b>	<i>log-id</i> — Specifies the event log ID to be initialized or rolled over. <b>Values</b> 1 to 100

### log-id

<b>Syntax</b>	<b>log-id</b> <i>log-id</i>
<b>Context</b>	clear>log
<b>Description</b>	Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.  This command is only applicable to event logs that are directed to file destinations and memory destinations.  SNMP, syslog, console, or session logs are not affected by this command.
<b>Parameters</b>	<i>log-id</i> — Specifies the event log ID to be initialized or rolled over. <b>Values</b> 1 to 100

### event-handling

<b>Syntax</b>	<b>event-handling</b>
---------------	-----------------------

---

<b>Context</b>	clear>log
<b>Description</b>	This command enables the context to clear Event Handling System (EHS) information.

## handler

<b>Syntax</b>	<b>handler</b> <i>event-handler-name</i>
<b>Context</b>	clear>log>event-handling
<b>Description</b>	This command clears the counters in the <b>show log event-handling handler</b> <i>handler-name</i> output. It does affect the global or aggregate counters shown using the <b>information</b> command.
<b>Parameters</b>	<i>handler-name</i> — Specifies the name of the event handler, up to 32 characters in length.

## information

<b>Syntax</b>	<b>information</b>
<b>Context</b>	clear>log>event-handling
<b>Description</b>	This command clears handler statistics in the <b>show log event-handling information</b> output.

### 6.9.2.3 Tools Commands

## all-subscriptions

<b>Syntax</b>	<b>all-subscriptions</b>
<b>Context</b>	tools>dump>log
<b>Description</b>	This command displays the list of CLI logs to which each CLI session is currently subscribed.
<b>Output</b>	The following is an example of all-subscriptions output.

#### Sample Output

```
=====
CLI log subscriptions of all CLI sessions
=====
Session ID      : 6
Type            : console
User            : admin
Login time      : 19OCT2017 08:24:14
Remote IP address: 192.168.102.122
```

```
Log ID      : 1
            : 2
            : 3
            : 4
            : 5
...
            : 20
-----
Session ID   : 25
Type        : telnet
User        : admin
Login time   : 19OCT2017 08:33:16
Remote IP address: 192.168.102.138
Log ID      : 1
            : 2
=====
```

Table 111 describes all-subscriptions output fields.

**Table 111      Output Parameters**

Label	Description
Session ID	Specifies the session ID.
Type	Specifies the type of session (console, telnet, and so on).
User	Specifies the name of the user.
Login time	Specifies the time the user logged in.
Remote IP address	Specifies the originating (client side) IP address of the session.
Log ID	Specifies the log ID.

subscriptions

- Syntax**      **subscriptions**
- Context**     tools>dump>log
- Description**    This command displays the list of active subscriptions for this CLI session only.
- Output**        The following is an example of subscriptions output.

**Sample Output**

```
=====
CLI logs this CLI session is subscribed to
=====
Log Id
-----
31
```



72

-----  
No. of subscriptions: 2  
=====

Table 112 describes subscriptions output fields.

**Table 112 Output Parameters**

Label	Description
No. of subscriptions	Specifies the number of active subscriptions.

## subscribe-to

<b>Syntax</b>	<b>subscribe-to log-id</b> <i>log-id</i>
<b>Context</b>	tools>perform>log
<b>Description</b>	This command subscribes the current CLI session to the specified CLI log. Log events for the specified log will be output in the current CLI session until the CLI session closes or an unsubscribe-from command is used.
<b>Parameters</b>	<i>log-id</i> — Specifies the log ID for which subscription is requested.
<b>Values</b>	1 to 101

## unsubscribe-from

<b>Syntax</b>	<b>unsubscribe-from log-id</b> <i>log-id</i>
<b>Context</b>	tools>perform>log
<b>Description</b>	This command cancels the subscription of the current CLI session to the specified CLI log.
<b>Parameters</b>	<i>log-id</i> — Specifies the log ID from which cancellation is requested.
<b>Values</b>	1 to 101



---

## 7 sFlow

### 7.1 sFlow Overview

Some Layer 2 network deployments collect statistics on physical Ethernet ports and on Layer 2 interfaces at a high-frequency using a push model to, among others, monitor traffic, diagnose network issues, and/or provide billing. SR OS supports cflowd and XML accounting; however, those mechanisms are either Layer 3-specific, or focus on providing statistics at extremely large scale (thus use a pull model and cannot support high-frequency counter updates). To meet the statistics collection requirements of such Layer 2 deployments, SR OS supports sFlow statistics export using sFlow version 5.

The following list gives the main caveats for sFlow support:

- sFlow data sources require multi-core line cards (IOM), enabling sFlow on a card that is not a multi-core is not blocked and can be detected by SNMP trap/log generated by sFlow
- To meet high-frequency export of counters, sFlow implementation is targeted for low per-port VLL/VPLS SAP scale only. The configuration is blocked if the per-port VLL/VPLS SAP limit exceeds sFlow limit. Contact your Nokia representative for per-platform scaling limits applicable.

---

## 7.2 sFlow Features

This section describes sFlow functionality supported in SR OS.

### 7.2.1 sFlow Counter Polling Architecture

When sFlow is enabled on an SR OS router, the system takes upon a role of an sFlow network device as described in sFlow protocol version 5. A single sFlow agent can be configured for counter polling (flow sampling is not supported). There is no support for sub-agents.

The sFlow agent sends sFlow data to an operator-configured sFlow receiver. A single receiver is supported with configurable primary and backup IPv4 or IPv6 UDP destination sockets for redundancy (each sFlow packet exported is duplicated to both sockets when both are configured). The receiver's UDP sockets can be reachable either in-band or out-of-band (default) and must both be IPv4 or IPv6. An operator can also set the maximum size of the sFlow datagrams. Operators are expected to set this value to avoid IP fragmentation (Datagrams exceeding the specified size are fragmented before handed to IP layer).

The sFlow agent manages all sFlow data sources in the system. SR OS supports sFlow data that are physical ports. When a port is configured as an sFlow data source, counters for that port and all VPLS and Epipe SAPs on that port are collected and exported using sFlow (see later on section for record format). Flow data sources can only be configured when an sFlow receiver is configured. To remove the sFlow receiver, all sFlow data sources must first be deconfigured at the port level.

Each data source is processed at a 15-second, non-configurable interval. If multiple data sources exist on a line card, the line card distributes the processing of each data source within a 15 second interval to avoid sFlow storms. When a timer expires to trigger a data source processing, data is collected for the physical port and for all VLL and VPLS SAPs on that port and exported using sFlow version 5 records as described in later subsections of this document. Each port and all SAP records for a given data source for a given interval are collected and sent with the counter sequence number and the timestamp value (the time value corresponds to the time counters were actually collected by a line card). The timestamp value uses line card's sysUptime value, which is synchronized with CPM time automatically by the system. A line card sends the counters to a CPM card, where sFlow UDP datagrams are created, sequenced with the CPM sequence number and sent to the receiver. If no UDP sockets are configured, no errors are generated because data is not sent. If no UDP sockets are reachable, the created UDP sFlow datagrams are dropped.



**Note:** Line cards will reset the counter record sequence numbers if, as a result of configuration or operational change, the return statistics no longer provide continuity with the previous interval. This may occur when:

- The card hard or soft resets
- The MDA resets
- The sFlow agent counter map changes



**Note:** The CPM will reset the sFlow datagram sequence numbers if, as a result of configuration or operational change, the sFlow datagram to be sent no longer provides continuity with the previous datagram. The following lists examples of when this takes place:

- HA switch
- CTL reboot
- Creation of an sFlow receiver

## 7.2.2 sFlow Support on Logical Ethernet Ports

sFlow data sources operate in a context of physical Ethernet port. To enable sFlow on Ethernet logical ports and their SAPs, an operator must explicitly enable sFlow on every physical Ethernet port that is a member of the given logical port. Currently only LAG logical ports are supported (including MC-LAG).



**Note:** sFlow configuration does not change automatically when a port is added or removed to or from a LAG.

For SAPs on a LAG, egress statistics will increment based on ports used by each SAP on LAG egress while ingress statistics will increment based on ports used by each SAP on LAG ingress unless LAG features like, for example, per-fp-ingress-queuing or per-fp-sap-optimization result in SAP statistics collection against a single LAG port.

If logical-level view is required, for example, per LAG statistics, a receiver is expected to perform data correlation based on per-physical port interface and SAP records exported for the given logical port's physical ports and their SAPs. sFlow data records contain information that allows physical ports/SAP records correlation to a logical port. See [sFlow Record Formats](#).



**Note:** Correlation of records must allow for small difference in timestamp values returned for member ports or SAP on a LAG because all ports run independent timestamps.

### 7.2.3 sFlow SAP Counter Map

To allow per SAP sFlow statistics export, operators must configure ingress and egress sFlow counter maps. The counter maps are required, because SR OS systems support more granular per policer/queue counters and not IF-MIB counters per VLL/VPLS SAPs. In an absence of a map configured, 0's will be returned in corresponding statistics records.

A single ingress and a single egress counter map are supported. The maps specify which ingress and which egress SAP QoS policy queue/policer statistics map to sFlow unicast, multicast, and broadcast counters returned in an sFlow SAP record. Multiple queues and/or policers can map to each of unicast, multicast, broadcast counters. A single queue/policer can only map to one type of traffic. Queues, policers configured in a SAP QoS policy but not configured in an sFlow map or vice-versa are ignored when sFlow statistics are collected.

### 7.2.4 sFlow Record Formats

Table 113 describes sFlow record used and exported:

**Table 113** sFlow Record Fields

Record	Field	Value
sFlow Datagram Header (SAP and port)	Datagram version	5
	Agent Address	Active CPM IPv4 address (from BoF)
	Sub-agent ID	0
	Sequence number	CPM inserted sFlow datagram sequence number
	SysUptime	sysUptime when the counters for records included in the datagram were collected by the line card
	NumSamples	Number of counter records in the datagram

**Table 113 sFlow Record Fields (Continued)**

Record	Field	Value
Counter header (SAP and Port)	Enterprise	0 (standard sFlow)
	sFlow Sample Type	4 (Expanded counter sample)
	Sample Length	sFlow packet size excluding header
	Sequence number	Line card-inserted sequence number
	Source ID Type	0
	Source ID Index	tmnxPortId of the physical port (sFlow data source)
	Counter records	Count of counter records in the datagram
Ethernet Interface Counters (EIC) – port (Ethernet Layer)	Enterprise	Statistics returned are based on dot3StatsEntry in EtherLike-MIB.mib. Statistics support may depend on hardware type.
	Format	
	Flow data length	
	Alignment Errors	
	FCS Errors	
	Single Collision Frames	
	Multiple Collision Frames	
	SQE Test Errors	
	Deferred Transmissions	
	Late Collisions	
	Excessive Collisions	
	Internal Mac Transmit Errors	
	Carrier Sense Errors	
	Frame Too Longs	
	Internal Mac Receive Errors	
	Symbol Errors	

**Table 113 sFlow Record Fields (Continued)**

Record	Field	Value
Generic Interface Counters (GIC) – port/ SAP	Enterprise	0 (standard sFlow)
	Format	1 (GIC)
	Flow data length	88
	ifIndex	Port: ifIndex (tmnxPortId) of phys port SAP: SapEncapValue - part of SAP SNMP key
	ifType	Port: 6 (EthernetCsmacd) SAP: 1 (Other)
	ifSpeed	Port: Port speed value SAP: <ul style="list-style-type: none"> <li>• top 32 bits: svcId for SAP (TIMETRA-SAP.mib)</li> <li>• lower 32 bits: sapPortId (TIMETRA-SAP.mib)</li> </ul> The values plus ifIndex in the record are SAP SNMP key. SapPortId is LAG's tmnxPortId for SAPs on a LAG and port's tmnxPortId for SAPs on physical port
	ifDirection	Derived from MAU MIB (0 = unknown, 1 = full duplex, 2 = half duplex, 3 = in, 4 = out)
	ifAdminStatus	0 (down) 1 (up)
	ifOperStatus	0 (down) 1 (up)
	Input Octets	Statistics return for port are based on ifEntry or ifXEntry in IF-MIB.mib as applicable. Statistics returned for SAPs are sum of counters based on the sFlow ingress/egress counter map configured.
	Input Packets	
	Input Multicast packets	
	Input Broadcast packets	
	Input Discarded packets	



**Table 113 sFlow Record Fields (Continued)**

Record	Field	Value
Generic Interface Counters (GIC) – port/ SAP (Continued)	Input Errors	Statistics return for port are based on ifEntry or ifXEntry in IF-MIB.mib as applicable. Statistics returned for SAPs are sum of counters based on the sFlow ingress/egress counter map configured.
	Input Unknown Protocol Packets	
	Output Octets	
	Output Packets	
	Output Multicast packets	
	Output Broadcast packets	
	Output Discarded packets	
	Output Errors	
	Promiscuous Mode	0 (FALSE)

**Notes:**

- 0 is returned for statistics that are not supported by a given hardware type.
- If required, CPM executes rollover logic to convert internal 64-bit counters to a 32-bit sFlowd counter returned.



## 7.3 sFlow Command Reference

The commands listed in this section apply to the 7950 XRS, 7750 SR-12e, and 7750 SR-7/12 platforms.

### 7.3.1 Command Hierarchies

- [System Commands](#)
- [Show Commands](#)

To enable sFlow collection, an operator must enable sFlow on physical Ethernet ports in addition to the following configuration. Refer to the Ethernet Port Commands section in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide* for the CLI required to enable sFlow on physical ports.

#### 7.3.1.1 System Commands

```
config
— sflow
— egress-counter-map {policer policer-id | queue queue-id} traffic-type {unicast |
multicast | broadcast} [create]
— no egress-counter-map {policer policer-id | queue queue-id}
— ingress-counter-map {policer policer-id | queue queue-id} traffic-type {unicast |
multicast | broadcast} [create]
— no ingress-counter-map {policer policer-id | queue queue-id}
— receiver receiver-name [create]
— no receiver
— ip-addr-primary ip-address[:port]
— no ip-addr-primary
— ip-addr-backup ip-address[:port]
— no ip-addr-backup
— max-data-size bytes
```

#### 7.3.1.2 Show Commands

```
show
— sflow
```



## 7.4 sFlow Configuration Command Descriptions

This section provides the sFlow configuration command descriptions.

### 7.4.1 Command Descriptions

The topics in this section include:

- [System Commands](#)
- [Show Commands](#)

#### 7.4.1.1 System Commands

The following commands apply to the 7950 XRS, 7750 SR-12e, and 7750 SR-7/12 platforms.

#### sflow

<b>Syntax</b>	<b>sflow</b>
<b>Context</b>	config>sflow
<b>Description</b>	This command enables context to configured sflow agent parameters.

#### egress-counter-map

<b>Syntax</b>	<b>egress-counter-map policer</b> <i>policer-id</i> <b>traffic-type</b> {unicast   multicast   broadcast} [create] <b>egress-counter-map queue</b> <i>queue-id</i> <b>traffic-type</b> {unicast   multicast   broadcast} [create] <b>no egress-counter-map policer</b> <i>policer-id</i> <b>no egress-counter-map queue</b> <i>queue-id</i>
<b>Context</b>	config>sflow
<b>Description</b>	This command configures the egress counter map for sFlow. The map must be configured so sFlow agent understands how to interpret data collected against SAP queues and policers. Multiple queues and policers can be mapped to the same <b>traffic-type</b> using separate line entries.

The **no** form of this command deletes a SAP policy queue/policer from the map.

- Parameters** *policer-id* — Specifies the policer ID in a SAP egress QoS policy. If the SAP policy does not have a policer with the specified ID, the map entry will be ignored for this SAP.
- Values** 1 to 8
- queue-id* — Specifies the queue ID in a SAP egress QoS policy. If the SAP policy does not have a queue with the specified ID, the map entry will be ignored for this SAP.
- Values** 1 to 8

## ingress-counter-map

- Syntax** **ingress-counter-map policer** *policer-id* **traffic-type** {unicast | multicast | broadcast} [create]  
**ingress-counter-map queue** *queue-id* **traffic-type** {unicast | multicast | broadcast} [create]  
**no ingress-counter-map policer** *policer-id*  
**no ingress-counter-map queue** *queue-id*
- Context** config>sflow
- Description** This command configures the ingress counter map for sFlow. The map must be configured so sFlow agent understands how to interpret data collected against SAP queues and policers. Multiple queues/policers can be mapped to the same **traffic-type** using separate line entries.
- The **no** form of this command deletes a SAP policy queue/policer from the map.
- Default** No mapping is created by default.
- Parameters** *policer-id* — Specifies the policer ID in a SAP ingress QoS policy. If the SAP policy does not have a policer with the specified ID, the map entry will be ignored for this SAP.
- Values** 1 to 32
- queue-id* — Specifies the queue ID in a SAP ingress QoS policy. If the SAP policy does not have a queue with the specified ID, the map entry will be ignored for this SAP.
- Values** 1 to 32

## receiver

- Syntax** **receiver** *receiver-name* [create]  
**no receiver**
- Context** config>sflow
- Description** This command creates an sFlow receiver context or enters existing sFlow receiver context for the sFlow agent.

The **no** form of this command deletes an existing sFlow receiver context.

**Default** No receivers are created by default.

**Parameters** *receiver-names* — String of up to 127 characters.

## ip-addr-primary

**Syntax** **ip-addr-primary** *ip-address[:port]*  
**no ip-addr-primary**

**Context** config>sflow>receiver

**Description** This command configures primary IPv4 or IPv6 destination address for the sFlow agent to send sFlow datagrams to. Optionally a destination port can also be configured (by default port 6343 is used).

The **no** form of this command deletes primary sFlow receiver destination.

**Default** no ip-addr-primary

**Parameters** *ip-address* — Specifies the IPv4 or IPv6 address to send the sFlow datagrams.

**Values**

a.b.c.d	(IPv4)
x:x:x:x:x:x:x	(IPv6)
[x:x:x:x:x:x:x]	(IPv6)
x - [0..FFFF]H	

*port* — Specifies the UDP destination port to send the sFlow datagrams.

**Values** 1 to 65535

## ip-addr-backup

**Syntax** **ip-addr-backup** *ip-address[:port]*  
**no ip-addr-backup**

**Context** config>sflow>receiver

**Description** This command configures back-up IPv4 or IPv6 destination address for the sFlow agent to send sFlow datagrams to. Optionally a destination port can also be configured (by default port 6343 is used).

The **no** form of this command deletes backup sFlow receiver destination.

**Default** no ip-addr-backup

---

**Parameters**    *ip-address* — Specifies the IPv4 or IPv6 address to send the sFlow datagrams to.

**Values**

a.b.c.d	(IPv4)
x:x:x:x:x:x:x	(IPv6)
[x:x:x:x:x:x:x]	(IPv6)
x - [0 to FFFF]H	

*port* — Specifies the UDP destination port to send the sFlow datagrams to.

**Values**        1 to 65535

## max-data-size

**Syntax**        **max-data-size** *bytes*

**Context**        config>sflow>receiver

**Description**    This configures the maximum data size for sFlow UDP datagrams sent to the collector.  
To restore default configuration, execute max-data-size 1400.

**Default**        max-data-size 1400

**Parameters**    *bytes* — Specifies the data size.

**Values**        200 to 1500



## 7.5 sFlow Show Command Descriptions

This section provides the sFlow show command descriptions.

### 7.5.1 Command Descriptions

The commands described in this section apply to the 7950 XRS, 7750 SR-12e, and 7750 SR-7/12 platforms.

The command outputs in this section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### 7.5.1.1 Show Commands

##### sflow

<b>Syntax</b>	<b>sflow</b>
<b>Context</b>	show>sflow
<b>Description</b>	This command displays the primary and backup receiver statistics, the mapping configuration and a summary of how many ports and SAPs have sFlow enabled.  <a href="#">Table 114</a> describes the show sflow output fields.
<b>Output</b>	The following is an example of Sflow information.

##### Sample Output

```
*B:bkvm10# show sflow
=====
sFlow Status
=====
Receiver           : pat
Max Data Size      : 312

IP Addr Primary    : 10.120.142.163:6343
Packets Sent       : 2572
Packet Errors      : 2
Last Packet Sent   : 07/08/2014 22:23:57nt

IP Addr Backup     : N/A
Packets Sent       : 0
Packet Errors      : 0
```

```

Last Packet Sent      : No Pkts sent
-----
Counter Pollers
-----
Port                  No. of SAPs
-----
1/1/2                 3
1/2/1                 0
-----
No. of sFlow counter pollers: 2
-----
Counter Mappings
-----
Direction            Policer/Queue  Traffic Type
-----
egress               queue 1      unicast
egress               queue 5      multicast
egress               queue 8      broadcast
ingress              policer 1    unicast
ingress              policer 6    multicast
ingress              policer 12   broadcast
-----
No. of sFlow counter mappings: 6
=====

```

**Table 114** Show Sflow Output Fields

Label	Description
<b>sFlow Status</b>	
Receiver	Displays the configured name for the sFlow receiver.
Max Data Size	The configured maximum data size for sFlow UDP packets.
IP Addr Primary	The primary IP address and destination port for sFlow receiver.
IP Addr Backup	The backup IP address and destination port for sFlow receiver.
Packets Sent	The number of packets sent successfully to the primary or backup receiver destination, since the destination was configured, CPM card HA switchover, or system reboot.
Packet Errors	The number of packets that could not be sent to the primary or backup receiver destination because of an error, since the destination was configured, CPM card HA switchover, or system reboot. An example of an error is destination IP not reachable.
Last Packet Sent	Displays the date and time of the last packet sent.

**Table 114 Show Sflow Output Fields (Continued)**

Label	Description
<b>Counter Pollers</b>	
Port	Displays the port on which sFlow is enabled.
No. of SAPs	The number of SAPs on the port with sFlow enabled.
No. of sFlow counter pollers	The number of sFlow counter pollers.
<b>Counter Mappings</b>	
Direction	Displays the direction of traffic (ingress or egress) the map entry applies to.
Policer/Queue	Displays the policer or queue instance being mapped by sFlow map.
Traffic type	Displays the type of sFlow traffic statistics (unicast, multicast or broadcast) that the policer/queue maps to.
No. of sFlow counter mappings	The number of entries in the sFlow ingress and egress counter map.



## 8 gRPC

gRPC is a modern, open-source, high-performance RPC framework that runs in any environment. In SR OS, this framework is used to implement the gRPC server, which can be then be used for configuration management or telemetry.

The gRPC transport service uses HTTP/2 bidirectional streaming between the gRPC client (the data collector) and the gRPC server (the SR OS device). A gRPC session is a single connection from the gRPC client to the gRPC server over the TCP/TLS port.

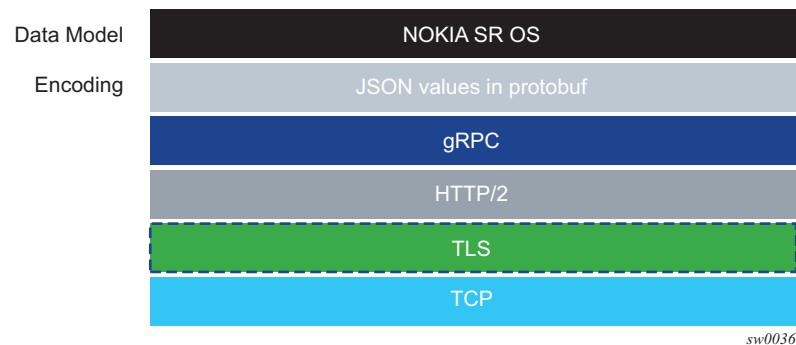
The gRPC service runs on port 57400 by default in SR OS. The service is not configurable.

A single gRPC server supports concurrent gRPC sessions and channels.

- There is a maximum of eight concurrent gRPC sessions for all of the gRPC clients.
- There is a maximum of 225 concurrent gRPC channels for all of the gRPC clients.

Figure 21 shows the gRPC protocol stack.

**Figure 21 Protocol Stack**



---

## 8.1 Security Aspects

### 8.1.1 TLS-Based Encryption

The gRPC server on SR OS can operate in two modes:

- without TLS encryption
- with TLS encryption

TLS encryption is used for added security. However, TLS encryption can be disabled in lab environments.

If TLS is not used, gRPC messages are not encrypted and user-names and passwords required in gRPC communication are visible to anyone capturing the packets. Therefore, Nokia recommends disabling TLS encryption only in a closed environment.

Before a gRPC connection will come up without TLS, the following conditions must both be met:

- no TLS server profile is assigned to the gRPC server
- the **allow-unsecure-connection** flag is set

The following summarizes the process of encryption:

- To use TLS encryption:
  - The gRPC session must be in an encrypted state.
  - If the gRPC client and gRPC server are unable to negotiate an encrypted gRPC session, the gRPC session fails and the gRPC server sends an error.
  - Fallback from an encrypted to an unencrypted gRPC session is not allowed.

For information about how to configure TLS with gRPC, see the [TLS](#) chapter.

### 8.1.2 Authentication

User authentication is based on following principles:

- Each RPC sent by the gRPC client carries a username and password.

- For the first RPC in the gRPC session, the gRPC server tries to authenticate the user using the specified authentication order, such as using the local user database, RADIUS, or TACACS+.

For example, if TACACS+ is first in the authentication order, the gRPC server sends a request to the TACACS+ server to authenticate the gRPC user.

- For the subsequent RPCs on that same authenticated gRPC session, the username and password are re-authenticated only if changed.
- When no username and password are provided with the RPC, the gRPC server returns an error.
- If the RPC user is changed, any active subscriber RPCs on that same gRPC session are terminated by the gRPC server.
- If the RPC password is changed, the active gRPC session will continue to exist until a different username and password is sent in a subsequent RPC, or the gRPC session is terminated.
- Each message is carried over a gRPC session that was previously encrypted; the session is not re-encrypted.
- SR OS device authentication
  - The gRPC clients do not share gRPC sessions. Each gRPC client starts a separate gRPC session.
  - When a gRPC session is established, the gRPC server certificates are verified by the gRPC client to ensure that every gRPC server is authenticated by the gRPC client.
  - If gRPC is shut down on the gRPC server and a gRPC client is trying to establish a gRPC session, the gRPC client will get an error for every RPC sent.
  - If gRPC is shut down on the gRPC server and a gRPC session is established, all active RPCs are gracefully terminated and an error is returned for every active RPC.

## 8.2 gNMI Service

gRPC Network Management Interface (gNMI) is a gRPC based protocol for network management functions, such as configuration and retrieval of information from network elements. In addition, it provides functionality necessary for supporting telemetry. gNMI service is specified in the OpenConfig forum.

### 8.2.1 gNMI Service Definitions

The SR OS gRPC server supports gNMI version 0.4.0, and in particular, the following RPC operations:

- Capability RPC
- Set/Get RPCs
- Subscribe RPC

#### 8.2.1.1 Capability Discovery

In gNMI service, the client discovers the capabilities of the gRPC server through a Capability-Discovery RPC, which consists of “CapabilityRequest” and “CapabilityResponse” messages.

During this message exchange, the gRPC server informs the client about following attributes:

- supported gNMI version
- supported models
- supported encodings

The SR OS server announces the supported models based on the configuration under **configure>system>management-interface>yang-modules**. The supported models includes the NOKIA-YANG or OpenConfig (OC) models.

The advertised module names and organizations are as follows:

- nokia-conf, org = "Nokia"
- nokia-state, org = "Nokia"
- openconfig, org = "OpenConfig working group" (as specified by the 'organization' in the YANG models)



- version - the version number will be defined as follows:
  - for NOKIA YANG models, the version number will correspond to an SR OS release number, for example, "16.0r1"
  - for OC YANG models, the version number will correspond to a version number defined in "oc-ext:openconfig-version" that is included in the respective YANG models
  - for OC-YANG models, including NOKIA deviations, the version number will correspond to an SR OS release number, for example, "16.0r1"

The following is an example of a “Capabilities Response Message”:

Going to send message of type gnmi.CapabilityResponse:

```
.gnmi_version: 0.4.0
.supported_encodings (1):
  .encoding: 0 = JSON
.supported_models (47):
  { .name: 'nokia-conf', .organization: 'Nokia', .version: '16.0.r1' }
  { .name: 'nokia-state', .organization: 'Nokia', .version: '16.0.r1' }
  { .name: 'openconfig-
bgp', .organization: 'OpenConfig working group', .version: '4.0.1' }
<snip>
  { .name: 'nokia-sr-openconfig-if-ethernet-
deviations', .organization: 'Nokia', .version: '16.0.r1' }
  { .name: 'nokia-sr-openconfig-if-ip-
deviations', .organization: 'Nokia', .version: '16.0.r1'..."
```

### 8.2.1.2 Get/Set RPC

Information is retrieved from the NE using GET RPC messages, which consists of “GetRequest” and “GetResponse” messages. The client asks for a given information by specifying following:

- A set of paths — all rules to a path definition apply, as specified in the gNMI specification
- Type — configuration, state, or operational data
- Encoding — in accordance to server advertisement during capability discovery
- Use\_models — this message will be ignored

There is an upper limit on the size of the “GetResponse” message. This limit cannot exceed 100MB. If the limit is exceeded, the SR OS gRPC server responds with an error message.

In order to modify the information in an NE element, a SET gRPC message is used. This gRPC supports three types of transactions:

- delete

- replace
- update

### 8.2.1.3 Subscribe RPC

A subscription is initiated from the gRPC client by sending a Subscribe RPC that contains a "SubscribeRequest" message to the gRPC server. A prefix can be specified to be used with all paths specified in the "SubscribeRequest". If a prefix is present, it is appended to the start of every path to provide a full path.

A subscription contains:

- a list of one or more paths. The following conditions apply:
  - A path represents the data tree as a series of repeated strings and elements. Each element represents a data tree node name and its associated attributes.
  - A path must be syntactically valid within the set of schema modules that the gRPC server supports.
  - The path list cannot be modified during the lifetime of the subscription.
  - If the subscription path is to a container node, all child leafs of that container node are considered to be subscribed to.
  - Any specified path must be unique within the list; paths cannot be repeated within the list. An error is returned if the same path is used more than one time in a single subscription.
  - A specified path does not need to pre-exist within the current data tree on the gRPC server. If a path does not exist, the gRPC server continues to monitor for the existence of the path. Assuming that the path exists, the gRPC server transmits telemetry updates.
  - The gRPC server does not send any data for a non-existent path; for example, if a path is non-existent at the time of subscription creation or if the path was deleted after the subscription was established.
  - The maximum number of paths for all subscriptions on a single SR OS device is 14400. A path using a wildcard is still considered a single path.
- a subscription mode of one of the following types:
  - ONCE mode — the server returns only one notification containing all information the client has subscribed to. In general, retrieving large amounts of information from the NE can be done using telemetry: "SubscribeRequest" message with ONCE subscription type.

- ON-CHANGE mode — the server returns notifications only when the value of the subscribed field changes. See [ON-CHANGE Subscription Mode](#) for more information.
- SAMPLE mode — the gRPC server sends notifications at the specified sampling interval
- TARGET\_DEFINED mode — means ON-CHANGE for all states supporting on-change notifications and SAMPLE mode for all other objects in the YANG tree
- a sample interval is supported for each path. If a sample interval of less than 10 s is specified, the gRPC server returns an error. If the sample interval is set to 0, the default value of 10 s is used. A sample interval is specified in nanoseconds (10 000 000 000 by default)

When a subscription is successfully initiated on the gRPC server, “SubscribeReponse” messages are sent from the gRPC server to the gRPC client. The “SubscribeResponse” message contains update notifications about the subscription's path list.

An update notification contains:

- a timestamp of the statistics collection time, represented in nanoseconds
- a prefix:
  - If a prefix is present, it is logically appended to the start of every path to provide the full path.
  - The presence of a prefix in the “SubscriptionResponse” message is not related to the presence of a prefix in the original “SubscriptionRequest” message. The prefix in the “SubscriptionResponse” message is optimized by the gRPC server.
- a list of updates (path and value pairs):
  - A path represents the data tree path as a series of repeated strings or elements, where each element represents a data tree node name and its associated attributes. See [Schema Paths](#) for more information.
  - The “TypedValue” message represents the data tree node's value where encoding is always “JSON”.

A sync response notification is sent one time, after the gRPC server sends all of the updates for the subscribed-to paths. The sync response must be set to “true” for the gRPC client to consider that the stream has synced one time. A sync response is used to signal the gRPC client that it has a full view of the subscribed-to data.

The gRPC server sends an error if required. The error contains a description of the problem.

### 8.2.1.3.1 ON-CHANGE Subscription Mode

SR OS supports ON-CHANGE subscription mode. This subscription mode indicates that Notification messages are sent as follows:

- after the “SubscriptionRequest” message is received
- every time the corresponding leaf value is changed

The notification message, as a response to an ON-CHANGE subscription, always contains the new value of the corresponding leaf, as defined in gNMI specification.

The ON-CHANGE subscription is supported for all configuration events as well as for selected state leafs. The **tools** command can display all state leafs supporting the ON-CHANGE subscription.

ON-CHANGE subscription is accepted for all valid paths. The server sends ON-CHANGE notifications only for leafs within this path that support ON-CHANGE notifications.

### 8.2.1.4 Schema Paths

Telemetry subscriptions include a set of schema paths used to identify which data nodes are of interest to the collector.

The paths in Telemetry Subscribe RPC requests follow the basic conventions described in the *OpenConfig gnmi-path-conventions.md* published on github.com (version 0.2.0 from February 24th, 2017).

A path consists of a set of path segments often shown with a “/” character as a delimiter; for example, /configure/router[router-instance=Base]/interface[interface-name=my-interface1]/description.

These paths are encoded as a set of individual string segments in gnmi.proto (without any “/” characters); for example, ["configure", "router[router-instance=Base]", "interface[interface-name=my-interface1]", "description"].

A path selects an entire subtree of the data model and includes all descendants of the node indicated in the path. [Table 115](#) describes the types of schema paths that are supported in SR OS telemetry.

**Table 115 Schema Paths**

Path example	Description
/configure/router[router-instance=Base]/interface[interface-name=abc]	Selects all config leafs of interface abc and all descendants.
/configure/router[router-instance=Base]/interface[interface-name=abc]/description	Selects only the description leaf of interface abc.
/state/router[router-instance=Base]/interface[interface-name=*]	Selects all state information for all base router interfaces using a wildcard in a single segment of a path.
/configure/router[router-instance=Base]/interface[interface-name=*]/description	Selects all state information for all base router interfaces using a wildcard in a single segment of a path.
/	The root path. This selects all config and state data from all models (in all namespaces) supported on the router. Encoded as "" in gRPC/gPB.

The following list describes types of telemetry paths that are not supported in SR OS.

- Wildcards for entire path segments are not supported.  
For example: /state/service/\*/oper-status
- If a wildcard is used for any key of a list, a wildcard must be used for all the keys of that list. In a single path segment, all the keys must either have specific values or all the keys must have wildcards. A mix of wildcards and specific values for different parts of a list key is not supported.  
For example:  
Supported:  
/a/b[key1=\*][key2=\*]/c[key1=foo]  
/a/b[key1=foo][key2=bar]/c[key1=\*]  
Not supported:  
/a/b[key1=foo][key2=\*]
- Functions such as "current()", "last()" and mathematical operators, such as stat<5 or octets>3 are not supported in paths. The "|" (OR operator, used to select multiple paths) is not supported.
- The "//" wildcard pattern is not supported.  
For example: /state//oper-status

The following list describes types of telemetry paths that are supported in SR OS.

- Wildcards in multiple segments of a path are supported.  
For example: /state/card[slot-number=\*/mda[mda-slot=\*]

## 8.2.2 gNMI Service Use Cases

The gNMI Service can be used for the following:

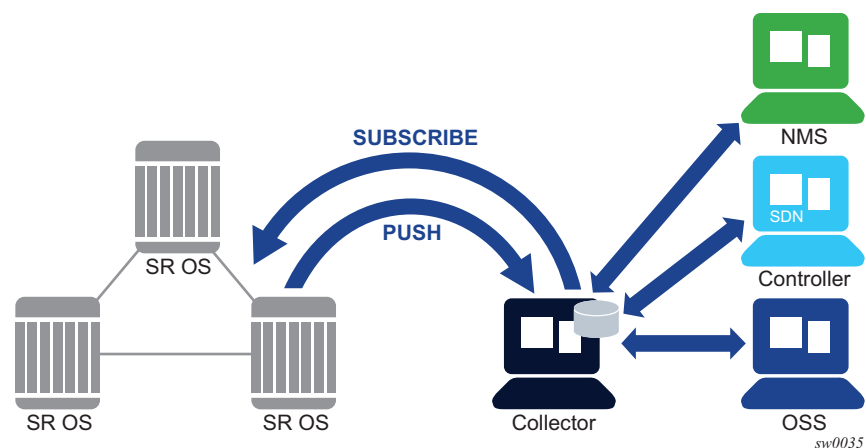
- Telemetry
- NE Configuration Management

### 8.2.2.1 Telemetry

Telemetry is a network monitoring and fault management framework. Telemetry is driven by the need to use fresh data obtained from the network to make fast networking decisions such as traffic optimization and preventative troubleshooting.

Unlike legacy monitoring platforms such as SNMP, telemetry does not only rely on continuously pulling data from the network devices. Instead, network devices push and stream data (such as statistics) continuously to data collectors based on subscriptions. The data collectors can then filter, analyze, store, and make decisions using the collected data from the network devices. [Figure 22](#) shows a telemetry application.

**Figure 22** Telemetry Application



### 8.2.2.1.1 Telemetry Examples

This section contains examples of Telemetry subscription requests and responses. The following examples are dumps of protobuf messages from a Python API. Formats may vary across different implementations.

#### Example 1 — Subscribe to a single path

```
2017-06-05 17:06:13,189 - SENT::SubscribeRequest
subscribe {
  subscription {
    path {
      element: "state"
      element: "router[router-instance=Base]"
      element: "interface[interface-name=test]"
      element: "statistics"
      element: "ip"
      element: "in-packets"
    }
    mode: SAMPLE
    sample_interval: 10000000000
  }
}

2017-06-05 17:06:13,190 - RCVD::SubscribeResponse
2017-06-05 17:06:23,492 - RCVD::Subscribe
2017-06-05 17:06:23,492 - update {
  timestamp: 1496675183491595139
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=test]"
    element: "statistics"
    element: "ip"
  }
  update {
    path {
      element: "in-packets"
    }
    val {
      json_val: ""0""
    }
  }
}

2017-06-05 17:06:23,494 - RCVD::Subscribe
2017-06-05 17:06:23,494 - sync_response: true

2017-06-05 17:06:33,589 - RCVD::Subscribe
2017-06-05 17:06:33,589 - update {
  timestamp: 1496675213491595139
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=test]"
    element: "statistics"
    element: "ip"
```

```

    }
    update {
      path {
        element: "in-packets"
      }
      val {
        json_val: ""28""
      }
    }
  }
  ....
  ....

```

### Example 2 — Subscribe to a single path with wildcard

2017-06-05 17:08:29,055 - SENT::SubscribeRequest

```

subscribe {
  subscription {
    path {
      element: "state"
      element: "router[router-instance=Base]"
      element: "interface[interface-name=*"
      element: "statistics"
      element: "ip"
      element: "in-packets"
    }
    mode: SAMPLE
    sample_interval: 30000000000
  }
}

```

2017-06-05 17:08:29,056 - RCVD::SubscribeResponse

2017-06-05 17:08:59,133 - RCVD::Subscribe

```

2017-06-05 17:08:59,133 - update {
  timestamp: 1496675339132056575
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=system]"
    element: "statistics"
    element: "ip"
  }
  update {
    path {
      element: "in-packets"
    }
    val {
      json_val: ""0""
    }
  }
}

```

2017-06-05 17:08:59,135 - RCVD::Subscribe

```

2017-06-05 17:08:59,135 - update {
  timestamp: 1496675339133006678
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=to_node_B]"
    element: "statistics"
  }
}

```



```

        element: "ip"
    }
    update {
        path {
            element: "in-packets"
        }
        val {
            json_val: ""0""
        }
    }
}
2017-06-05 17:08:59,135 - RCVD::Subscribe
2017-06-05 17:08:59,135 - update {
    timestamp: 1496675339133006678
    prefix {
        element: "state"
        element: "router[router-instance=Base]"
        element: "interface[interface-name=to_node_D]"
        element: "statistics"
        element: "ip"
    }
    update {
        path {
            element: "in-packets"
        }
        val {
            json_val: ""0""
        }
    }
}
2017-06-05 17:08:59,136 - RCVD::Subscribe
2017-06-05 17:08:59,136 - sync_response: true

2017-06-05 17:09:29,139 - RCVD::Subscribe
2017-06-05 17:09:29,139 - update {
    timestamp: 1496682569121314
    prefix {
        element: "state"
        element: "router[router-instance=Base]"
        element: "interface[interface-name=system]"
        element: "statistics"
        element: "ip"
    }
    update {
        path {
            element: "in-packets"
        }
        val {
            json_val: ""0""
        }
    }
}
2017-06-05 17:09:29,142 - RCVD::Subscribe
2017-06-05 17:09:29,142 - update {
    timestamp: 1496682569124342
    prefix {
        element: "state"
        element: "router[router-instance=Base]"
        element: "interface[interface-name=to_node_B]"
    }
}

```

```

        element: "statistics"
        element: "ip"
    }
    update {
        path {
            element: "in-packets"
        }
        val {
            json_val: ""0""
        }
    }
}
2017-06-05 17:09:29,145 - RCVD::Subscribe
2017-06-05 17:09:29,145 - update {
    timestamp: 1496682569127344
    prefix {
        element: "state"
        element: "router[router-instance=Base]"
        element: "interface[interface-name=to_node_D]"
        element: "statistics"
        element: "ip"
    }
    update {
        path {
            element: "in-packets"
        }
        val {
            json_val: ""0""
        }
    }
}
....
....

```

### Example 3: Subscribe to more than one path

```

2017-01-24 12:54:18,228 - SENT::SubscribeRequest
subscribe {
    subscription {
        path {
            element: "state"
            element: "router[router-instance=Base]"
            element: "interface[interface-name=to_node_B]"
        }
        mode: SAMPLE
        sample_interval: 30000000000
    }
    subscription {
        path {
            element: "state"
            element: "router[router-instance=Base]"
            element: "mpls"
            element: "statistics"
            element: "lsp-egress-stats[lsp-name=lsp_to_dest_f]"
        }
        mode: SAMPLE
        sample_interval: 30000000000
    }
}

```

```
}
```

#### Example 4: Subscribe to a list with wildcard

```
2017-01-24 13:45:30,947 - SENT::SubscribeRequest
subscribe {
  subscription {
    path {
      element: "state"
      element: "router[router-instance=Base]"
      element: "interface[interface-name=*"
    }
    mode: SAMPLE
    sample_interval: 30000000000
  }
}
```

#### Example 5: Subscribe to path where the object did not exist before subscription

```
2017-01-24 13:53:50,165 - SENT::SubscribeRequest
subscribe {
  subscription {
    path {
      element: "state"
      element: "router[router-instance=Base]"
      element: "interface[interface-name=to_node_B]"
    }
    mode: SAMPLE
    sample_interval: 30000000000
  }
}
```

```
2017-01-24 13:53:50,166 - RCVD::SubscribeResponse
2017-01-24 13:54:20,169 - RCVD::Subscribe
2017-01-24 13:54:20,169 - sync_response: true
```

```
2017-01-24 13:54:50,174 - RCVD::Subscribe
2017-01-24 13:54:50,174 - update {
  timestamp: 1485262490169309451
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=to_node_B]"
  }
  update {
    ...
    ...
  }
}
```

#### Example 6: Subscribe to a path where the object existed before subscription then was deleted after subscription

```
2017-01-24 14:00:41,292 - SENT::SubscribeRequest
subscribe {
```

```

subscription {
  path {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=to_node_B]"
  }
  mode: SAMPLE
  sample_interval: 30000000000
}

2017-01-24 14:00:41,294 - RCVD::SubscribeResponse
2017-01-24 14:01:11,295 - RCVD::Subscribe
2017-01-24 14:01:11,295 - update {
  timestamp: 1485262871290064704
  prefix {
    element: "state"
    element: "router[router-instance=Base]"
    element: "interface[interface-name=to_node_B]"
  }
  update {
    ...
    ...
  }
}
2017-01-24 14:01:11,359 - RCVD::Subscribe
2017-01-24 14:01:11,359 - sync_response: true

2017-01-24 14:01:41,293 - RCVD::Subscribe

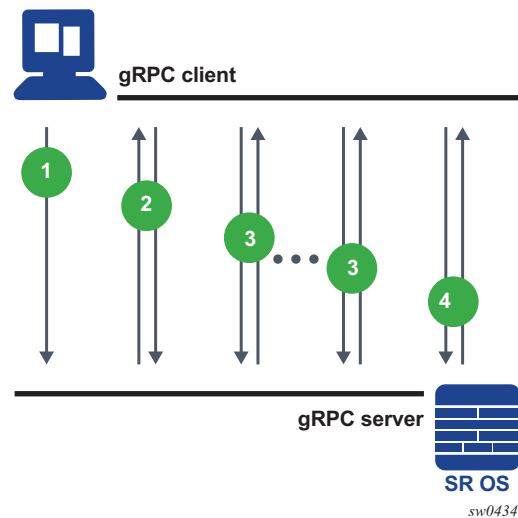
2017-01-24 14:02:11,296 - RCVD::Subscribe

```

### 8.2.2.2 NE Configuration Management

[Figure 23](#) shows NE configuration and information retrieval using the gNMI service.

**Figure 23 NE Configuration and Information Retrieval using gNMI Service**



In the context of gNMI, every SET RPC appears as an single commit operation, regardless of the number of paths included in the message. Both, NOKIA and OC models are supported by gNMI SET/GET RPC.

An example of the SET RPC command (including the response message from the gRPC server) follows:

```
gNMI_rpc - DEBUG - SENT::SetRequest
prefix {
}
update {
  path {
    elem {
      name: "configure"
    }
    elem {
      name: "system"
    }
  }
  val {
    json_val: {"location": "zurich"}
  }
}
gMI_rpc - DEBUG - RCVD::SetResponse
prefix {
}
response {
  path {
    elem {
```

```

        name: "configure"
      }
      elem {
        name: "system"
      }
    }
  }
  op: UPDATE
}

```

An example of the GET RPC command (including the response message from the gRPC server) follows:

```

gNMI_rpc - INFO - SENT::GetRequest GET140550212650064
path {
  elem {
    name: "configure"
  }
  elem {
    name: "system"
  }
  elem {
    name: "location"
  }
}
type: CONFIG
2017-12-06 12:17:28,639 - gMI_rpc - INFO -
  RCVD::GetResponse GET140550212650064
notification {
  timestamp: 1512559048634751055
  update {
    path {
      elem {
        name: "configure"
      }
      elem {
        name: "system"
      }
      elem {
        name: "location"
      }
    }
    val {
      json_val: "zurich"
    }
  }
}
}

```

---

## 8.3 gRPC Command Reference

The commands listed in this section apply to the 7950 XRS, 7750 SR-12e, and 7750 SR-7/12 platforms.

### 8.3.1 Command Hierarchies

#### 8.3.1.1 System Commands

```
config
  — system
    — grpc
      — max-msg-size number
      — no max-msg-size
      — no shutdown
      — tls-server-profile name
      — no tls-server-profile
```

#### 8.3.1.2 QoS Commands

```
config
  — router
    — sgt-qos
      — application
        — grpc
          — dscp {dscp-value | dscp-name}
```





## 8.4 Telemetry Configuration Command Descriptions

This section provides Telemetry configuration command descriptions.

### 8.4.1 Command Descriptions

The topics in this section include:

- [System Commands](#)
- [QoS Commands](#)

#### 8.4.1.1 System Commands

##### grpc

<b>Syntax</b>	<b>grpc</b>
<b>Context</b>	config>system config>router>sgt-qos>application
<b>Description</b>	This command enables the context to configure gRPC parameters.

##### max-msg-size

<b>Syntax</b>	<b>max-msg-size</b> <i>number</i> <b>no max-msg-size</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command configures the maximum gRPC rx message size.
<b>Default</b>	max-msg-size 512
<b>Parameters</b>	<i>number</i> — Specifies the maximum message size in megabytes. <b>Values</b> 1 to 1024

## shutdown

<b>Syntax</b>	<b>no shutdown</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command disables the gRPC server. The <b>shutdown</b> command is not blocked if there are active gRPC sessions. Shutting down gRPC will terminate all active gRPC sessions.

## tls-server-profile

<b>Syntax</b>	<b>tls-server-profile</b> <i>name</i> <b>no tls-server-profile</b>
<b>Context</b>	config>system>grpc
<b>Description</b>	This command provides the TLS profile name to use for the gRPC server.
<b>Parameters</b>	<i>name</i> — Specifies the TLS server profile name up to 32 characters in length.

### 8.4.1.2 QoS Commands

## dscp

<b>Syntax</b>	<b>dscp</b> { <i>dscp-value</i>   <i>dscp-name</i> }
<b>Context</b>	config>router>sgt-qos>application>grpc
<b>Description</b>	This command configures a DiffServ Code Point (DSCP) name to be used for gRPC.
<b>Parameters</b>	<p><i>dscp-value</i> — Represents the gRPC traffic class.</p> <p><b>Values</b> 0 to 63</p> <p><i>dscp-name</i> — Represents the gRPC traffic class.</p> <p><b>Values</b> none be ef cp1 cp2 cp3 cp4 cp5 cp6 cp7 cp9 cs1 cs2 cs3 cs4 cs5 nc1 nc2 af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cp11 cp13 cp15 cp17 cp19 cp21 cp23 cp25 cp27 cp29 cp31 cp33 cp35 cp37 cp39 cp41 cp42 cp43 cp44 cp45 cp47 cp49 cp50 cp51 cp52 cp53 cp54 cp55 cp57 cp58 cp59 cp60 cp61 cp62 cp63</p>

## 8.5 gRPC Show, Admin Command Reference

This section provides the gRPC show and admin command descriptions.

### 8.5.1 Command Hierarchies

- [Show Commands](#)
- [Tools Commands](#)
- [Admin Commands](#)

#### 8.5.1.1 Show Commands

```

show
  — system
    — telemetry
      — grpc
        — subscription
        — subscription subscription-id [paths]

show
  — router
    — sgt-qos
      — application
        — grpc
          — dscp
  
```

#### 8.5.1.2 Tools Commands

```

tools
  — dump
  — system
    — cpm-http-redirect redirect statistics
    — cpm-http-redirect redirect summary
    — cpm-http-redirect tcp sessions
    — cpm-http-redirect tcp settings
    — cpm-http-redirect tcp statistics
    — Telemetry
      — on-change-paths
      — on-change-paths {open-config | nokia}
  
```

### 8.5.1.3 Admin Commands

```
admin
  — system
    — telemetry
      — grpc
        — subscription subscription-id cancel
        — subscription cancel-all
```

## 8.5.2 Command Descriptions

- [Show Commands](#)
- [Admin Commands](#)

### 8.5.2.1 Show Commands

grpc

- Syntax**      **grpc**
- Context**     show>system>telemetry
- Description**    This command displays the gRPC server status.
- Output**        The following output displays gRPC server information.
- [Table 116](#) describes gRPC fields.

**Sample Output**

```
=====
gRPC Server
=====
Administrative State      : Disabled
Operational State        : Down
=====
```

**Table 116      Show System gRPC Output Fields**

Labels	Description
gRPC Server	

**Table 116** Show System gRPC Output Fields (Continued)

Labels	Description
Administrative State	Enabled — Displays that gRPC is enabled. Disabled — Displays that gRPC is disabled.
Operational State	Up — Displays that gRPC is operational. Down — Displays that gRPC is not operational.

## subscription

<b>Syntax</b>	<b>subscription</b> <i>subscription-id</i> [ <b>paths</b> ] <b>subscription</b>
<b>Context</b>	show>system>telemetry>grpc
<b>Description</b>	This command displays the active telemetry gRPC subscriptions.
<b>Parameters</b>	<i>subscription-id</i> — A unique subscription ID or number that is assigned by the SR OS gRPC server to each active telemetry subscription. <b>paths</b> — Indicates that the <b>show</b> command output includes all paths with the respective subscription ID information.
<b>Output</b>	The following output describes the telemetry gRPC subscription fields.

### Sample Output

```
A:node-6>show>system>telemetry>grpc# subscription
=====
Telemetry gRPC subscriptions
=====
Id           User           Mode           Port
Destination
-----
1            admin          stream         49648
      192.99.5.0
-----
No. of gRPC Telemetry subscriptions: 1
=====

A:node-6>show>system>telemetry>grpc# subscription 2
=====
Telemetry gRPC subscription
=====
Subscription-id : 2
User            : admin
Destination     : 192.168.110.252
Port            : 54309
=====
```

```

A:node-6>show>system>telemetry>grpc# subscription 1 paths
=====
Telemetry gRPC subscription
=====
Subscription id      : 1
User                 : admin
Destination          : 192.99.5.0
Port                 : 49648
Subscription mode    : stream
-----
Paths
-----
Path                 : /state/router[router-instance=]/interface[interface-
                      name=]/ipv4/oper-state
Path mode            : on-change
Sample interval      : 10000 ms
Finished samples     : 1
Deferred samples     : 0
Total collection time : 6 ms
Min collection time  : 6 ms
Avg collection time  : 6 ms
Max collection time  : 6 ms
-----
No. of paths         : 1
=====

```

## grpc

**Syntax**     **grpc**

**Context**    show>router>sgt-qos>application

**Description** This command displays the gRPC router status.

## dscp

**Syntax**     **dscp**

**Context**    show>router>sgt-qos>application>grpc

**Description** This command displays the configured DSCP name or value for gRPC.

### 8.5.2.2 Tools Commands

## cpm-http-redirect redirect statistics

**Syntax**     **cpm-http-redirect redirect statistics**

**Context** tools>dump>system

**Description** This command displays system level statistics for all redirected TCP sessions in **optimized-mode**. These include the following:

- Close requests to TCP: TCP layer requested to send a FIN
- Abort requests to TCP: error in the received packet and the TCP layer needs to send a RST
- Data requests to TCP: number of redirects sent to the TCP layer
- Connections deleted: number of connections closed without a successful redirect performed
- HTTP GET parse errors: formatting error in the HTTP request
- HTTP GET process errors: HTTP GET is formatted properly but the redirect still fails. Example: system unable to find a corresponding host
- HTTP Response dropped: communication error; the redirect failed to be sent to the TCP layer

```
A# tools dump system cpm-http-redirect redirect statistics
=====
CPM HTTP Redirect statistics
=====
Close requests to TCP                : 2
Abort requests to TCP                : 0
Data requests to TCP                 : 2
Requests rejected - out of memory    : 0
Connections deleted                  : 0
HTTP GET parse errors                : 0
HTTP GET process errors               : 0
HTTP Response dropped                : 0
```

## cpm-http-redirect redirect summary

**Syntax** cpm-http-redirect redirect summary

**Context** tools>dump>system

**Description** This command displays the summary statistics of **cpm-http-redirect optimized-mode** for the total number of host and connections currently in use. It, also, allows to compare the current system utilization with the maximum system scale.

```
A# tools dump system cpm-http-redirect summary
=====
CPM HTTP Redirect summary
=====
Actual number of hosts                : 0
Actual number of connections          : 0
Number of hosts created in the last second : 0
Number of connections created in the last second : 0
=====
```

## cpm-http-redirect tcp sessions

<b>Syntax</b>	<b>cpm-http-redirect tcp sessions</b>
<b>Context</b>	tools>dump>system
<b>Description</b>	<p>This command displays the system level TCP session state information of the <b>cpm-http-redirect optimized-mode</b> for currently opened sessions. Specifically, the following are displayed:</p> <ul style="list-style-type: none"> <li>• New: Syn received and Syn-Ack not sent</li> <li>• SYN: Syn-Ack sent and waiting for Ack</li> <li>• ESTABLISHED: Ack received and waiting for data</li> <li>• FIN: FIN sent and waiting for Fin-Ack</li> <li>• Delete: Sum of all currently open connections at this time, representing the connections to be deleted</li> <li>• HTTP Response dropped: communication error; the redirect failed to be sent to the TCP layer</li> </ul>

All current sessions are counted both in the state where they belong, such as 'New', 'Syn', 'Established', 'Fin', and in the sum 'Delete' count.

```
A# tools dump system cpm-http-redirect tcp sessions
=====
CPM HTTP Redirect TCP session information
=====
TCP sessions in new state                : 0
TCP sessions in state SYN                 : 0
TCP sessions in state ESTABLISHED         : 0
TCP sessions in state FIN                 : 0
TCP sessions in delete state              : 0
=====
```

## cpm-http-redirect tcp settings

<b>Syntax</b>	<b>cpm-http-redirect tcp settings</b>
<b>Context</b>	tools>dump>system
<b>Description</b>	<p>This command displays the system level TCP settings of the <b>cpm-http-redirect optimized-mode</b>. These settings can be further controlled using <b>tools perform</b> commands.</p>

```
Dut-A# tools dump system cpm-http-redirect tcp settings
data-retransmissions 1
data-timeout 20
established-timeout 100
fin-ack-retransmissions 1
fin-ack-timeout 15
max-connections 500
max-connections-per-host 20
max-hosts 500
```



```
syn-ack-retransmissions 1
syn-ack-timeout 20
```

## cpm-http-redirect tcp statistics

<b>Syntax</b>	<b>cpm-http-redirect tcp statistics</b>
<b>Context</b>	tools>dump>system
<b>Description</b>	This command displays the system level TCP statistics of the <b>cpm-http-redirect optimized-mode</b> for all sessions.

```
A# tools dump system cpm-http-redirect tcp statistics
=====
CPM HTTP Redirect TCP statistics (only nonzero values shown)
=====
Packets forwarded                               : 25
TCP segments received                           : 8
Not a TCP segment                               : 17
Packets offered to redirect                     : 2
SYN received                                    : 2
FIN,ACK received                                : 2
ACK received                                    : 4
Valid TCP packets received                      : 8
Received packets                               : 25
Received packets with a connection              : 8
Connection creations                           : 2
Connection deletions                           : 2
SYN processed                                  : 2
SYN,ACK processed                              : 2
SYN,ACK with data processed                    : 2
FIN,ACK processed                              : 2
FIN,ACK with wrong sequence number             : 2
=====
```

## Telemetry

<b>Syntax</b>	<b>telemetry</b>
<b>Context</b>	tools>dump>system
<b>Description</b>	This command enables the telemetry context.

## on-change-paths

<b>Syntax</b>	<b>on-change-paths</b> <b>on-change-paths {open-config   nokia}</b>
<b>Context</b>	tools>dump>system>telemetry

**Description** This command lists all paths supporting on-change notifications. The keywords **open-config** and **nokia** indicate which model should be used as a reference for the output.

**Parameters** **open-config** — Indicates that the open-config model will be used as the output reference.

**nokia** — Indicates that the Nokia model will be used as the output reference.

## Output

### Sample Output

```
A:node-6# tools dump system telemetry on-change-paths nokia
=====
Nokia on-change state paths
=====
/state/log/log-id/oper-state
/state/port/ethernet/lldp/dest-mac/remote-system/chassis-id
/state/port/ethernet/lldp/dest-mac/remote-system/chassis-id-subtype
/state/port/ethernet/lldp/dest-mac/remote-system/remote-port-id
/state/port/ethernet/lldp/dest-mac/remote-system/remote-port-id-subtype
/state/port/ethernet/lldp/dest-mac/remote-system/port-description
/state/port/ethernet/lldp/dest-mac/remote-system/system-enabled-capabilities
/state/port/ethernet/lldp/dest-mac/remote-system/system-supported-capabilities
/state/port/ethernet/lldp/dest-mac/remote-system/system-description
/state/port/ethernet/lldp/dest-mac/remote-system/system-name
/state/port/ethernet/lldp/dest-mac/remote-system/mgmt-address/interface-subtype
/state/port/ethernet/lldp/dest-mac/remote-system/mgmt-address/interface-id
/state/port/ethernet/lldp/dest-mac/remote-system/mgmt-address/object-identifier
/state/router/interface/if-oper-status
/state/router/isis/interface/level/oper-metric/ipv4-unicast
/state/router/isis/interface/level/oper-metric/ipv6-unicast
/state/router/isis/interface/level/oper-metric/ipv4-multicast
/state/router/isis/interface/level/oper-metric/ipv6-multicast
/state/router/mppls/lsp/oper-state
/state/router/mppls/lsp/primary/mbb/last-mbb/type
/state/router/mppls/lsp/primary/mbb/last-mbb/end-time
/state/router/mppls/lsp/primary/mbb/last-mbb/metric
/state/router/mppls/lsp/primary/mbb/last-mbb/state
/state/router/mppls/lsp/primary/mbb/last-mbb/signaled-bw
/state/router/mppls/lsp/secondary/mbb/last-mbb/type
/state/router/mppls/lsp/secondary/mbb/last-mbb/end-time
/state/router/mppls/lsp/secondary/mbb/last-mbb/metric
/state/router/mppls/lsp/secondary/mbb/last-mbb/state
/state/router/mppls/lsp/secondary/mbb/last-mbb/signaled-bw
/state/service/ies/interface/if-oper-status
/state/service/vprn/interface/if-oper-status
/state/service/vprn/log/log-id/oper-state
/state/system/lldp/chassis-id
/state/system/lldp/chassis-id-subtype
/state/system/lldp/system-name
/state/system/lldp/system-description
/state/system/telemetry/grpc/subscription/path/deferred-collection-count
=====
```

---

### 8.5.2.3 Admin Commands

#### subscription

<b>Syntax</b>	<b>subscription</b> <i>subscription-id</i> <b>cancel</b>
<b>Context</b>	admin>system>telemetry>grpc
<b>Description</b>	This command cancels an active Telemetry subscription.
<b>Parameters</b>	<i>subscription-id</i> — Specifies the ID of the Telemetry subscription to cancel.
<b>Values</b>	0 to 4294967295

#### subscription cancel-all

<b>Syntax</b>	<b>subscription cancel-all</b>
<b>Context</b>	admin>system>telemetry>grpc
<b>Description</b>	This command cancels all active Telemetry subscriptions.



---

## 9 TLS

### 9.1 TLS Overview

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

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

In certain situations, the server can request a certificate from the client to authenticate it. The client has a certificate (called a Trust Anchor) from the certificate authority (CA) which is used to authenticate server certificate and its DS. After the client provides a digitally signed certificate to the server and both parties are authenticated, the encryption PDUs can then be transmitted.

When SR OS is acting as a server and it requests a certificate from the client, the client must provide the certificate. If the client fails to provide a certificate for authentication, SR OS will terminate the TLS session. The server TLS settings can be configured to not request certificates, in which case the client is not obligated to send the server a certificate for authentication.

- encryption and authentication of application PDUs

After the clients and server have been successfully authenticated, the cipher suite is negotiated between the server and clients, and the PDUs will be encrypted based on the agreed cipher protocol.

## 9.2 TLS Server Interaction with Applications

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

After successful negotiation and handshake, the TLS will be operationally up, and the TLS will notify the application which will begin transmitting PDUs. These PDUs will be encrypted using TLS based on the agreed ciphers. If, at any point, the TLS becomes operationally down, the application should stop transmitting PDUs.

For example, a TLS connection with the gMI application would operate as follows:

1. A TLS server profile is assigned to the gMI application.
2. gMI stops sending clear text PDUs because a TLS server profile has been assigned and TLS is not ready to encrypt.
3. The TLS server begins the handshake.
4. Authentication occurs at the TLS layer.
5. The TLS server and TLS client negotiate ciphers.
6. SALTs are negotiated for the symmetric key. A SALT is a seed for creating AES encryption keys.
7. When negotiations are successfully completed, the handshake finishes and gMI is notified.
8. TLS becomes operationally up, and gMI can resume transmitting PDUs. Until TLS becomes operationally up, gMI PDUs arriving from the client are dropped on ingress.

### 9.2.1 TLS Application Support

Table 117 lists the applications that support TLS.

**Table 117** TLS Application Support

Application	TLS Server Supported	TLS Client Supported
LDAP	NO	YES
gRPC	YES	NO

## 9.3 TLS Handshake

Figure 24 shows the TLS handshake.

**Figure 24** TLS Handshake

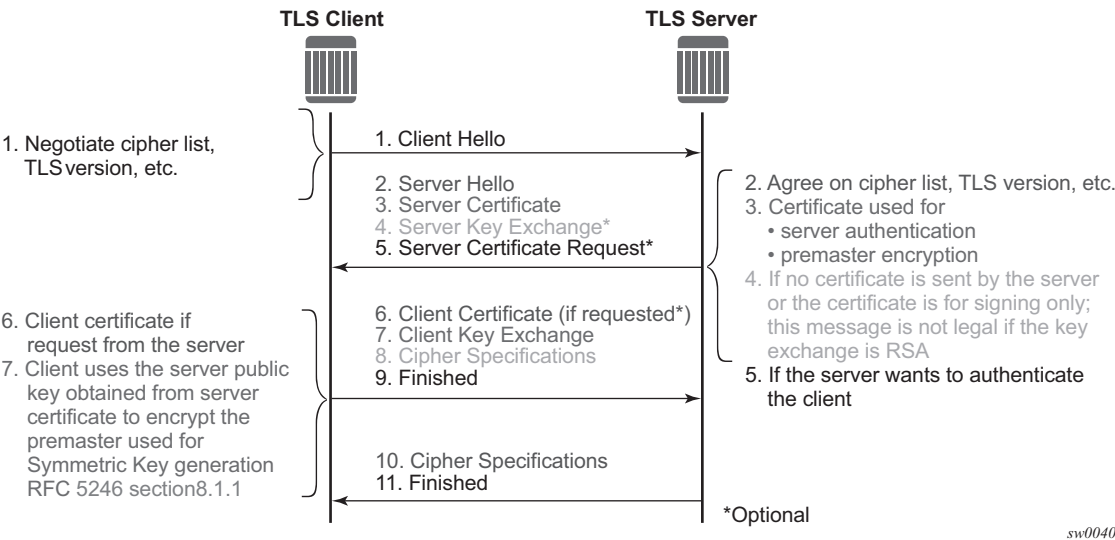


Table 118 further describes the steps in the TLS handshake.

**Table 118** TLS Handshake Step Descriptions

Step	Description
1	The TLS handshake begins with the client Hello message. This message includes the cipher list that the client wishes to use and negotiate, among other information.
2	The TLS server sends back a server Hello message, along with the first common cipher found on both the client cipher list and the server cipher list. This agreed cipher will be used for data encryption.
3	The TLS server continues by sending a server certificate message, where the server provides a certificate to the client so that the client can authenticate the server identity. The public key of this certificate (RSA key) can also be used for encryption of the symmetric key seed that will be used by the client and server to create the symmetric encryption key. This occurs only if the PKI is using RSA for asymmetric encryption.
4	Server key exchange is not supported by SR OS. SR OS only uses RSA keys; Diffie-Hellman key exchange is not supported.

**Table 118 TLS Handshake Step Descriptions (Continued)**

Step	Description
5	The server can optionally be configured to request a certificate from the client to authenticate the client.
6	If the server has requested a certificate, the client should provide a certificate using a client certificate message. If the client does not provide a certificate, the server will drop the TLS session.
7	The client uses the server public RSA key that was included in the server certificate to encrypt a seed used for creating the symmetric key. This seed is used by the client and server to create the identical symmetric key for encrypting and decrypting the data plane traffic.
8	The client sends a cipher spec to switch encryption to this symmetric key.
9	The client successfully finishes the handshake.
10	The server sends a cipher spec to switch encryption to this symmetric key.
11	The server successfully finishes the handshake.

After a successful handshake, TLS will be operationally up, and applications can then use it for application encryption.



---

## 9.4 TLS Client Certificate

TLS protocol is used for authentication, and as such, the server can ask to authenticate the client via PKI. If the server requests authentication from the client, the client must provide an X.509v3 certificate to the server so that it can be authenticated via the digital signature of its client. SR OS allows the configuration of an X.509v3 certificate for TLS clients. When the server requests a certificate via the server's Hello message, the client will transmit its certificate to the server using a client certificate message.

---

## 9.5 TLS Symmetric Key Rollover

SR OS supports key rollover via HelloRequest messages as detailed in RFC 5246, section 7.4.1.1. Some applications have a longer live time than other applications, in which case SR OS can use a timer that prompts the HelloRequest negotiation for the symmetric key rollover. This timer is configurable using CLI.

If an application does not support the HelloRequest message, the **no tls-re-negotiate-timer** command should be configured under the **config>system>security>tls** context. For example, the gRPC application does not support HelloRequest messages.

When **no tls-re-negotiate-timer** is configured, the HelloRequest message is not generated, and symmetric keys are not renegotiated.

---

## 9.6 Supported TLS Ciphers

As shown in [Figure 24](#), TLS negotiates the supported ciphers between the client and the server.

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

The 7750 SR supports the following ciphers as a TLS client or TLS server:

- `tls-rsa-with-null-md5`
- `tls-rsa-with-null-sha`
- `tls-rsa-with-null-sha256`
- `tls-rsa-with3des-ede-cbc-sha`
- `tls-rsa-with-aes128-cbc-sha`
- `tls-rsa-with-aes256-cbc-sha`
- `tls-rsa-with-aes128-cbc-sha256`
- `tls-rsa-with-aes256-cbc-sha256`

## 9.7 SR OS Certificate Management

SR OS implements a centralized certificate management protocol that can be used by TLS and IPSec. Refer to the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter Guide* for information about the configuration of the certificates and the corresponding protocols, such as OCSP, CMPv2, and CRL.

The main certificate configurations are:

- certificate configuration and management, configured using the **admin>certificate** commands
- PKI configuration (including creating a CA profile), configured using the **config>system>security>pki** commands

The two main configuration sub-trees for certificates are displayed below. See [Public Key Infrastructure \(PKI\) Commands](#) for more information.

**CLI Syntax:**

```
admin>certificate
  clear-ocsp-cache
  cmpv2
  crl-update
  display
  export
  gen-keypair
  gen-local-cert-req
  import
  reload

config>system>security>pki
  [no] ca-profile
  certificate-display-format
  [no] certificate-expiration-warning
  [no] crl-expiration-warning
  [no] maximum-cert-chain-depth
```

### 9.7.1 Certificate Profile

The certificate profile is available for both the TLS server and the TLS client. The **cert-profile** command is configured for the server or client to transmit the provider certificate and its DS to the peer so that the peer can authenticate it via the **trust-anchor** and CA certificate.

---

Multiple provider certificates can be configured on SR OS; however, SR OS currently uses the smallest index as the active provider certificate, and will only send the certificate to the peer.

## 9.7.2 TLS Server Authentication of the Client Certificate CN Field

If the client provides a certificate upon request by the server, SR OS checks the certificate's common name (CN) field against local CN configurations. The CN is validated via the client IPv4/IPv6 address or FQDN.

If **cn-authentication** is not enabled, SR OS will not authenticate via the CN field and will only rely on certificate signature authentication.

## 9.7.3 CN Regexp Format

CN entries are configured by using the **config>system>security>pki>common-name-list** command. Entries should use regular expression (regexp), FQDN, or the IP address.

For information about regexp, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*, "CLI Usage".

## 9.8 Operational Guidelines

### 9.8.1 Server Authentication Behavior

Following the Hello messages, the server sends its certificate in a certificate message if it is to be authenticated. If required, a ServerKeyExchange message may also be sent. Refer to RFC 5246, section 7.3, for more information about the authentication behavior on the LDAP server.

The **trust-anchor-profile** command determines whether or not the server must be authenticated by the client.

**CLI Syntax:**

```
config>system>security>tls
      client-tls-profile ldap create
      [no] trust-anchor-profile
```



**Note:** If the **trust-anchor-profile** is configured and the **ca-certificate** or **ca-profile** is missing from this **trust-anchor-profile**, the TLS connection will fail and an “unknown\_ca” error will be generated, as per RFC 5246 section 7.2.2.

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

- a. If **trust-anchor-profile** is configured under the TLS **client-tls-profile** context, the server must be authenticated via the **trust-anchor-profile** command before a trusted connection is established between the server and the client.
- b. If there is no **trust-anchor-profile** under the **client-tls-profile** context, the trusted connection can be established without server authentication. The RSA key of the certificate will be used for public key encryption, requiring basic certificate checks to validate the certificate. These basic checks are:
  - time validity—the certificate is checked to ensure that it is neither expired nor not yet valid
  - certificate type—the certificate is not a CA certificate
  - keyUsage extension—if present, this must contain a digital signature and key encryption
  - host verification—the IP address or DNS name of the server is looked up, if available (for LDAP, only the IP address is used), in the common name (cn) or subjectAltName extension. This is to verify that the certificate was issued to that server and not to another.

---

## 9.8.2 Client TLS Profile and Trust Anchor Behavior and Scale

SR OS allows the creation of client TLS profiles, which can be assigned to applications such as LDAP to encrypt the application layer.

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

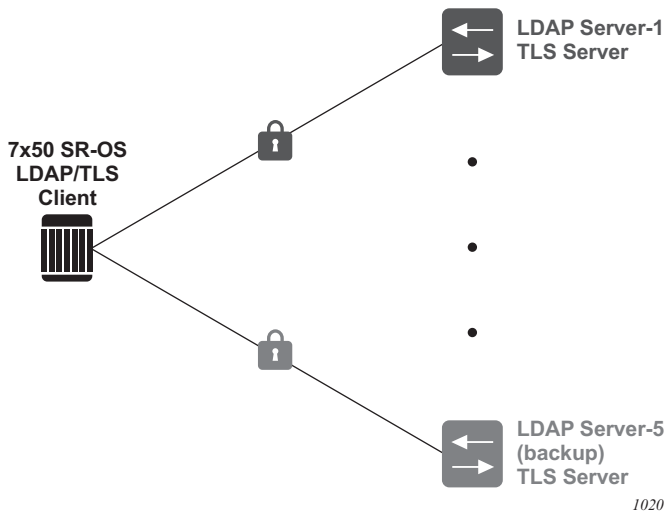
The client TLS profile must be assigned to an application for it to start encrypting. Up to 16 client TLS profiles can be configured. Because each of these client TLS profiles needs a trust anchor profile to authenticate the server, up to 16 trust anchor profiles can be configured. A trust anchor profile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

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

## 9.9 LDAP Redundancy and TLS

LDAP supports up to five redundant (backup) servers, as shown in [Figure 25](#) and the configuration examples below. Depending on the **timeout** and **retry** configurations, if an LDAP server is determined to be out of service or operationally down, SR OS will switch to the redundant servers. SR OS will select the LDAP server with the next largest configured server index.

**Figure 25** LDAP and TLS Redundancy



### Configuration of Server-1:

```
A*:SwSim14>config>system>security>ldap# info
public-key-authentication
server 1 create
address 1.1.1.1
ldap-server "active-server"
tls-profile "server-1-profile"

A*:SwSim14>config>system>security>tls# info
client-tls-profile "server-1-profile" create
cipher-list "to-active-server"
trust-anchor-profile "server-1-ca"
no shutdown
exit
```

### Configuration of Server-5 (backup):

```
A*:SwSim14>config>system>security>ldap# info
public-key-authentication
server 5 create
address 5.5.5.1
```



---

```
        ldap-server "backup-server-5"  
        tls-profile "server-5-profile"  
  
A*:SwSim14>config>system>security>tls# info  
    client-tls-profile "server-5-profile" create  
    cipher-list "to-backup-server-5"  
    trust-anchor-profile "server-5-ca"  
    no shutdown  
    exit
```

Each LDAP server can have its own TLS profile, each of which can have its own configuration of **trust-anchor** and **cipher-list**. For security reasons, the LDAP servers may be in different geographical areas and, as such, each will be assigned its own server certificate and trust anchor. The design is open to allow the user to mix and match all components.



## 9.10 Basic TLS Configuration

Basic TLS server configuration must have the following:

- a cipher list created using the **config>system>security>tls>server-cipher-list** command, and assigned to the TLS server profile using the **config>system>security>tls>server-tls-profile>cipher-list** command
- a certificate profile created using the **config>system>security>tls>cert-profile** command, and assigned to the TLS server profile using the **config>system>security>tls>server-tls-profile>cert-profile** command

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

TLS imports the trust anchor certificate for (TLS) peer certificate authentication and public key retrieval.

The following displays the CLI syntax for TLS:

**CLI Syntax:**

```
config>system>security>tls
    cert-profile profile-name [create]
    no cert-profile profile-name
    client-cipher-list name [create]
    no client-cipher-list name
    client-tls-profile name [create]
    no client-tls-profile name
    server-cipher-list name [create]
    no server-cipher-list name
    server-tls-profile name [create]
    no server-tls-profile name
    trust-anchor-profile name [create]
    no trust-anchor-profile name
```

The following displays a TLS configuration example.

```
config>system>security>tls# info
-----
trust-anchor-profile "server-1-ca" create
trust-anchor "tls-server-1-ca"
exit
client-cipher-list "to-active-server" create
cipher 1 name tls-rsa-with-aes256-cbc-sha256
cipher 2 name tls-rsa-with-aes128-cbc-sha256
cipher 3 name tls-rsa-with-aes256-cbc-sha
exit
client-tls-profile "server-1-profile" create
```

---

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

-----

---

## 9.11 Common Configuration Tasks

### 9.11.1 Configuring a Server TLS Profile

The following displays the CLI syntax for a server TLS profile.

**CLI Syntax:**

```
config>system>security>tls
    server-tls-profile name [create]
    no server-tls-profile name
    authenticate-client
        trust-anchor-profile ca-profile-name
    no trust-anchor-profile
    cert-profile name
    no cert-profile
    cipher-list name
    no cipher-list
    [no] shutdown
    tls-re-negotiate-timer [0 to 65000]
    no tls-re-negotiate-timer
```

### 9.11.2 Configuring a Client TLS Profile

The following displays the CLI syntax for a client TLS profile, which also configures the server authentication behavior:

**CLI Syntax:**

```
config>system>security>tls
    client-tls-profile name [create]
    no client-tls-profile name
    trust-anchor-profile name
    no trust-anchor-profile
```

### 9.11.3 Configuring a TLS Client or TLS Server Certificate

The following displays the CLI syntax for TLS certificate management:

**CLI Syntax:**

```
config>system>security>tls
    cert-profile profile-name [create]
    no cert-profile profile-name
    entry entry-id [create]
    no entry entry-id
```

```

        cert cert-filename
        no cert
        key key-filename
        no key
        [no] send-chain
            [no] ca-profile name
        [no] shutdown
    client-tls-profile name [create]
    no client-tls-profile name
        cert-profile name
        no cert-profile
    server-tls-profile name [create]
    no server-tls-profile name
        cert-profile name
        no cert-profile

```

## 9.11.4 Configuring a TLS Trust Anchor

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

```

CLI Syntax:  config>system>security>pki
                  [no] ca-profile
                  certificate-display-format
                  [no] certificate-expiration-warning hours
                  [no] crl-expiration-warning
                  [no] maximum-cert-chain-depth

                  config>system>security>tls
                  [no] trust-anchor-profile
                  [no] client-tls-profile
                  [no] cipher-list
                  [no] shutdown
                  [no] trust-anchor-profile-profile

```

The following displays a TLS trust anchor configuration example:

```

*B:SeGW-1>config>system>security>pki# info
-----
    ca-profile "tls-server-1-ca" create
    cert-file "tls-1-Root-CERT"
    crl-file "tls-1-CRL-CERT"
    no shutdown
    exit
-----
*A:SwSim8>config>system>security>tls# info
-----
    trust-anchor-profile "server-1-ca" create
    trust-anchor "tls-server-1-ca"

```

---

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





## 9.12 TLS Command Reference

### 9.12.1 Command Hierarchies

- [Security TLS Commands](#)
- [LDAP TLS Profile Commands](#)
- [Admin Commands](#)

#### 9.12.1.1 Security TLS Commands

```

config
  — system
    — security
      — tls
        — cert-profile profile-name [create]
        — no cert-profile profile-name
          — entry entry-id [create]
          — no entry entry-id
            — cert cert-filename
            — no cert
            — key key-filename
            — no key
            — [no] send-chain
              — [no] ca-profile name
              — [no] shutdown
        — client-cipher-list name [create]
        — no client-cipher-list name
          — cipher index name cipher-suite-code
          — no cipher index
        — client-tls-profile name [create]
        — no client-tls-profile name
          — cert-profile name
          — no cert-profile
          — cipher-list name
          — no cipher-list
          — [no] shutdown
          — trust-anchor-profile name
          — no trust-anchor-profile
        — server-cipher-list name [create]
        — no server-cipher-list name
          — cipher index name cipher-suite-code
          — no cipher index
        — server-tls-profile name [create]
        — no server-tls-profile name
          — authenticate-client

```

- **trust-anchor-profile** *name*
- **no trust-anchor-profile**
- **cert-profile** *name*
- **no cert-profile**
- **cipher-list** *name*
- **no cipher-list**
- **[no] shutdown**
- **tls-re-negotiate-timer** *timer-min*
- **no tls-re-negotiate-timer**
- **trust-anchor-profile** *name* [**create**]
- **no trust-anchor-profile** *name*
- **[no] trust-anchor** *ca-profile-name*

### 9.12.1.2 LDAP TLS Profile Commands

- ```

config
  — system
    — security
      — ldap
        — server server-index [create]
        — no server server-index
          — tls-profile tls-profile-name
          — no tls-profile

```

### 9.12.1.3 Admin Commands

- ```

admin
  — certificate
    — reload type {cert | key | cert-key-pair} filename protocol protocol [key-file filename]

```

## 9.12.2 Command Descriptions

This section provides the CLI command descriptions.

- [Security TLS Commands](#)
- [LDAP TLS Profile Commands](#)
- [Admin Commands](#)

---

### 9.12.2.1 Security TLS Commands

#### tls

<b>Syntax</b>	<b>tls</b>
<b>Context</b>	config>system>security
<b>Description</b>	This command configures TLS parameters.

#### cert-profile

<b>Syntax</b>	<b>cert-profile</b> <i>profile-name</i> [ <b>create</b> ] <b>no cert-profile</b> <i>profile-name</i>
<b>Context</b>	config>system>security>tls
<b>Description</b>	<p>This command configures TLS certificate profile information. The certificate profile contains the certificates that are sent to the TLS peer (server or client) to authenticate itself. It is mandatory for the TLS server to send this information. The TLS client may optionally send this information upon request from the TLS server.</p> <p>The <b>no</b> form of the command deletes the specified TLS certificate profile.</p>
<b>Parameters</b>	<p><i>profile-name</i> — Specifies the name of the TLS certificate profile, up to 32 characters in length.</p> <p><b>create</b> — Keyword used to create the TLS certificate profile.</p>

#### entry

<b>Syntax</b>	<b>entry</b> <i>entry-id</i> [ <b>create</b> ] <b>no entry</b> <i>entry-id</i>
<b>Context</b>	config>system>security>tls>cert-profile
<b>Description</b>	<p>This command configures an entry for the TLS certificate profile. A certificate profile may have up to eight entries. Currently, TLS uses the entry with the smallest ID number when responding to server requests.</p> <p>The <b>no</b> form of the command deletes the specified entry.</p>
<b>Parameters</b>	<p><i>entry-id</i> — Specifies the identification number of the TLS certificate profile entry.</p> <p><b>Values</b> 1 to 8</p> <p><b>create</b> — Keyword used to create the TLS certificate profile entry.</p>

---

## cert

<b>Syntax</b>	<b>cert</b> <i>cert-filename</i> <b>no cert</b>
<b>Context</b>	config>system>security>tls>cert-profile>entry
<b>Description</b>	This command specifies the file name of an imported certificate for the <b>cert-profile</b> entry.  The <b>no</b> form of the command removes the certificate.
<b>Default</b>	no cert
<b>Parameters</b>	<i>cert-filename</i> — Specifies the file name of the TLS certificate, up to 95 characters in length.

## key

<b>Syntax</b>	<b>key</b> <i>key-filename</i> <b>no key</b>
<b>Context</b>	config>system>security>tls>cert-profile>entry
<b>Description</b>	This command specifies the file name of an imported key for the <b>cert-profile</b> entry.  The <b>no</b> form of the command removes the key.
<b>Default</b>	no key
<b>Parameters</b>	<i>key-filename</i> — Specifies the file name of the key.

## send-chain

<b>Syntax</b>	<b>[no] send-chain</b>
<b>Context</b>	config>system>security>tls>cert-profile>entry
<b>Description</b>	This command enables the sending of certificate authority (CA) certificates, and enters the context to configure send-chain information.  By default, the system only sends the TLS server certificate or TLS client certificate specified by the <b>cert</b> command. If CA certificates are to be sent using send-chain, they must be in the chain of certificates specified by the <b>config&gt;system&gt;security&gt;pki&gt;ca-profile</b> command. The specification of the send-chain is not necessary for a working TLS profile if the TLS peer has the CA certificate used to sign the server or client certificate in its own trust anchor.

For example, given a TLS client running on SR OS, the ROOT CA certificate resides on the TLS server, but the subsequent SUB-CA certificate needed to complete the chain resides within SR OS. The **send-chain** command allows these SUB-CA certificates to be sent from SR OS to the peer to be authenticated using the ROOT CA certificate that resides on the peer.

The **no** form of the command disables the send-chain.

**Default** no send-chain

## ca-profile

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

**Context** config>system>security>tls>cert-profile>entry>send-chain

**Description** This command enables a certificate authority (CA) certificate in the specified CA profile to be sent to the peer. Up to seven configurations of this command are permitted in the same entry.

The **no** form of the command disables the transmission of a CA certificate from the specified CA profile.

**Parameters** *name* — Specifies the name of the certificate authority profile, up to 32 characters in length.

## shutdown

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

**Context** config>system>security>tls>cert-profile

**Description** This command disables the certificate profile. When the certificate profile is disabled, it will not be sent to the TLS server.

The **no** form of the command enables the certificate profile and allows it to be sent to the TLS server.

**Default** shutdown

## client-cipher-list

**Syntax** **client-cipher-list** *name* [**create**]  
**no client-cipher-list** *name*

**Context** config>system>security>tls

---

<b>Description</b>	This command creates a cipher list that the client sends to the server in the client Hello message. It is a list of ciphers that are supported and preferred by the SR OS to be used in the TLS session. The server matches this list against the server cipher list. The most preferred cipher found in both lists is chosen.
<b>Parameters</b>	<i>name</i> — Specifies the name of the client cipher list, up to 32 characters in length. <b>create</b> — Keyword used to create the client cipher list.

## cipher

<b>Syntax</b>	<b>cipher</b> <i>index name cipher-suite-code</i> <b>no cipher</b> <i>index</i>
<b>Context</b>	config>system>security>tls>client-cipher-list config>system>security>tls>server-cipher-list
<b>Description</b>	This command configures the cipher suite to be negotiated by the server and client.
<b>Parameters</b>	<i>index</i> — Specifies the index number. The index number provides the location of the cipher in the negotiation list, with the lower index numbers being higher in the negotiation list and the higher index numbers being at the bottom of the list.  <b>Values</b> 1 to 255  <i>cipher-suite-code</i> — Specifies the cipher suite code.  <b>Values</b> <ul style="list-style-type: none"> <li>tls-rsa-with-null-md5</li> <li>tls-rsa-with-null-sha</li> <li>tls-rsa-with-null-sha256</li> <li>tls-rsa-with-3des-ede-cbc-sha</li> <li>tls-rsa-with-aes128-cbc-sha</li> <li>tls-rsa-with-aes256-cbc-sha</li> <li>tls-rsa-with-aes128-cbc-sha256</li> <li>tls-rsa-with-aes256-cbc-sha256</li> </ul>

## client-tls-profile

<b>Syntax</b>	<b>client-tls-profile</b> <i>name</i> [ <b>create</b> ] <b>no client-tls-profile</b> <i>name</i>
<b>Context</b>	config>system>security>tls
<b>Description</b>	This command configures the TLS client profile to be assigned to applications for encryption.
<b>Parameters</b>	<i>name</i> — Specifies the name of the client TLS profile, up to 32 characters in length. <b>create</b> — Keyword used to create the client TLS profile.

---

## cert-profile

<b>Syntax</b>	<b>cert-profile</b> <i>name</i> <b>no cert-profile</b>
<b>Context</b>	config>system>security>tls>client-tls-profile
<b>Description</b>	<p>This command assigns a TLS certificate profile to be used by the TLS client profile. This certificate is sent to the server for authentication of the client and public key.</p> <p>The <b>no</b> form of the command removes the TLS certificate profile assignment.</p>
<b>Parameters</b>	<i>name</i> — Specifies the name of the TLS certificate profile, up to 32 characters in length.

## cipher-list

<b>Syntax</b>	<b>cipher-list</b> <i>name</i> <b>no cipher-list</b>
<b>Context</b>	config>system>security>tls>client-tls-profile
<b>Description</b>	This command assigns the cipher list to be used by the TLS client profile for negotiation in the client Hello message.
<b>Parameters</b>	<i>name</i> — Specifies the name of the cipher list.

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>security>tls>client-tls-profile config>system>security>tls>server-tls-profile
<b>Description</b>	This command administratively enables or disables the TLS profile. If the TLS profile is shut down, the TLS operational status will be down. Therefore, if the TLS profile is shut down, any application using TLS should not attempt to send any PDUs.

## trust-anchor-profile

<b>Syntax</b>	<b>trust-anchor-profile</b> <i>name</i> <b>no trust-anchor-profile</b>
<b>Context</b>	config>system>security>tls>client-tls-profile config>system>security>tls>server-tls-profile>authenticate-client
<b>Description</b>	This command assigns the trust anchor used by this TLS profile to authenticate the server or client.

The **no** form of the command removes the configured trust anchor profile.

**Parameters**    *name* — Specifies the name of the trust anchor profile.

## server-cipher-list

**Syntax**        **server-cipher-list** *name* [**create**]  
                 **no server-cipher-list** *name*

**Context**        config>system>security>tls

**Description**    This command creates the cipher list that is compared against cipher lists sent by the client to the server in the client hello message. The list contains all ciphers that are supported and desired by SR OS for use in the TLS session. The first common cipher found in both the server and client cipher lists will be chosen. As such, the most desired ciphers should be added at the top of the list.

The **no** form of the command removes the cipher list.

**Parameters**    *name* — Specifies the name of the server cipher list, up to 32 characters in length.  
                 **create** — Keyword used to create the server cipher list.

## server-tls-profile

**Syntax**        **server-tls-profile** *name* [**create**]  
                 **no server-tls-profile** *name*

**Context**        config>system>security>tls

**Description**    This command creates a TLS server profile. This profile can be used by applications that support TLS for encryption. The applications should not send any PDUs until the TLS handshake has been successful.

The **no** form of the command removes the TLS server profile.

**Parameters**    *name* — Specifies the name of the TLS server profile, up to 32 characters in length.  
                 **create** — Keyword used to create the TLS server profile.

## authenticate-client

**Syntax**        **authenticate-client**

**Context**        config>system>security>tls>server-tls-profile

**Description**    This command enters the context to configure client authentication parameters.



## cert-profile

<b>Syntax</b>	<b>cert-profile</b> <i>name</i> <b>no cert-profile</b>
<b>Context</b>	config>system>security>tls>server-tls-profile
<b>Description</b>	This command assigns a TLS certificate profile to be used by the TLS server profile. This certificate is sent to the client for authentication of the server and public key.  The <b>no</b> form of the command removes the TLS certificate profile assignment.
<b>Parameters</b>	<i>name</i> — Specifies the name of the TLS certificate profile, up to 32 characters in length.

## cipher-list

<b>Syntax</b>	<b>cipher-list</b> <i>name</i> <b>no cipher-list</b>
<b>Context</b>	config>system>security>tls>server-tls-profile
<b>Description</b>	This command assigns a cipher list to be used by the TLS server profile. This cipher list is used to find matching ciphers with the cipher list that is received from the client.  The <b>no</b> form of the command removes the cipher list.
<b>Parameters</b>	<i>name</i> — Specifies the name of the cipher list, up to 32 characters in length.

## tls-re-negotiate-timer

<b>Syntax</b>	<b>tls-re-negotiate-timer</b> <i>timer-min</i> <b>no tls-re-negotiate-timer</b>
<b>Context</b>	config>system>security>tls>server-tls-profile
<b>Description</b>	This command configures the timed interval after which the server is triggered to send a Hello request message to all clients and force a renegotiation of the symmetric encryption key. When an interval of 0 is configured, the server will never send a hello request message.
<b>Default</b>	tls-re-negotiate-timer 0
<b>Parameters</b>	<i>timer-min</i> — Specifies the interval, in minutes, after which the server is triggered to send a Hello request message.  <b>Values</b> 0 to 65000

## trust-anchor-profile

<b>Syntax</b>	<b>trust-anchor-profile</b> <i>name</i> [ <b>create</b> ] <b>no trust-anchor-profile</b> <i>name</i>
<b>Context</b>	config>system>security>tls
<b>Description</b>	This command configures a trust anchor profile to be used in the TLS profile. The trust anchor is used for authentication of the server certificate.
<b>Parameters</b>	<i>name</i> — Specifies the name of the trust anchor profile, up to 32 characters in length. <b>create</b> — Keyword used to create the trust anchor profile.

## trust-anchor

<b>Syntax</b>	[ <b>no</b> ] <b>trust-anchor</b> <i>ca-profile-name</i>
<b>Context</b>	config>system>security>tls>trust-anchor-profile
<b>Description</b>	This command configures a trust anchor with a CA profile used by the TLS profile. Up to eight CA profiles can be configured under the trust anchor. TLS will read the CA profiles one by one to try to authenticate the server certificate.
<b>Parameters</b>	<i>ca-profile-name</i> — Specifies the name of the TLS trust anchor, up to 32 characters in length.

### 9.12.2.2 LDAP TLS Profile Commands

## server

<b>Syntax</b>	<b>server</b> <i>server-index</i> [ <b>create</b> ] <b>no server</b> <i>server-index</i>
<b>Context</b>	config>system>security>ldap
<b>Description</b>	This command adds or removes an LDAP server.
<b>Parameters</b>	<i>server-index</i> — Specifies the server index. <b>Values</b> 1 to 5 <b>create</b> — Keyword used to create the server index.

## tls-profile

<b>Syntax</b>	<b>tls-profile</b> <i>tls-profile-name</i> <b>no tls-profile</b>
<b>Context</b>	config>system>security>ldap>server
<b>Description</b>	This command assigns a TLS profile to the LDAP application. When a TLS profile is assigned, the LDAP application will send encrypted PDUs from the client to the LDAP server. If TLS is operationally down, the LDAP application should not send any PDUs.
<b>Parameters</b>	<i>tls-profile-name</i> — Specifies the name of the TLS client transport profile.

### 9.12.2.3 Admin Commands

## reload

<b>Syntax</b>	<b>reload type</b> { <b>cert</b>   <b>key</b>   <b>cert-key-pair</b> } <i>filename protocol protocol</i> [ <b>key-file</b> <i>filename</i> ]
<b>Context</b>	admin>certificate
<b>Description</b>	This command manually reloads the certificate or key cache.
<b>Parameters</b>	<p><b>type</b> — Specifies what item will be reloaded.</p> <p><b>cert</b> — Specifies that a certificate cache will be reloaded.</p> <p><b>key</b> — Specifies that a key cache will be reloaded.</p> <p><b>cert-key-pair</b> — Specifies that a paired certificate and key cache will be reloaded.</p> <p><i>filename</i> — Up to 95 characters.</p> <p><i>protocol</i> — Specifies which protocol the certificate will be reloaded for.</p> <p><b>Values</b>      ipsec, tls</p>



# 9.13 TLS Show Command Reference

## 9.13.1 Command Hierarchies

- [Show Commands](#)

### 9.13.1.1 Show Commands

```
show
  — system
    — security
      — tls
          — cert-profile name association
          — cert-profile [name]
          — cert-profile name entry entry
          — client-tls-profile [client-tls-profile]
          — client-tls-profile client-tls-profile association
          — server-tls-profile [server-tls-profile]
          — server-tls-profile server-tls-profile association
          — trust-anchor-profile [trust-anchor-profile]
          — trust-anchor-profile trust-anchor-profile association
```

## 9.13.2 Command Descriptions

- [Show Commands](#)

### 9.13.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

tls

<b>Syntax</b>	tls
<b>Context</b>	show>system>security
<b>Description</b>	This command enables the context to display TLS-related information.

cert-profile

<b>Syntax</b>	<b>cert-profile</b> [ <i>name</i> ] <b>cert-profile</b> <i>name</i> <b>association</b> <b>cert-profile</b> <i>name</i> <b>entry</b> <i>entry</i>
<b>Context</b>	show>system>security>tls
<b>Description</b>	This command displays information about server and client profiles that are using this certificate profile.
<b>Parameters</b>	<i>entry</i> — Specifies a certificate profile entry number for which to display information. <b>Values</b> 1 to 8 <i>name</i> — Specifies the name of a certificate profile for which to display information.

client-tls-profile

<b>Syntax</b>	<b>client-tls-profile</b> [ <i>client-tls-profile</i> ] <b>client-tls-profile</b> <i>client-tls-profile</i> <b>association</b>
<b>Context</b>	show>system>security>tls
<b>Description</b>	This command displays TLS client profile information
<b>Parameters</b>	<i>client-tls-profile</i> — Specifies the client TLS profile, up to 32 characters maximum.
<b>Output</b>	The following output is an example of TLS client profile information.

Sample Output

```
*A:Dut-C> show system security tls client-tls-profile
=====
Client Profile Information
=====
Name                               AdminState   OperState
-----
ctp                                up           up
ctp-alt1                           up           up
ctp-alt2                           up           up
=====

*A:Dut-C> show system security tls client-tls-profile "ctp"
=====
Client Profile Entry "ctp"
=====
Cipher List Name                   : cl_all
Trust Anchor Profile Name         : tap
=====
```

## server-tls-profile

<b>Syntax</b>	<b>server-tls-profile</b> [ <i>server-tls-profile</i> ] <b>server-tls-profile</b> <i>server-tls-profile</i> <b>association</b>
<b>Context</b>	show>system>security>tls
<b>Description</b>	This command displays TLS server profile information.
<b>Parameters</b>	<i>server-tls-profile</i> — Specifies the name of a TLS server profile for which to display information, up to 32 characters maximum.

## trust-anchor-profile

<b>Syntax</b>	<b>trust-anchor-profile</b> [ <i>trust-anchor-profile</i> ] <b>trust-anchor-profile</b> <i>trust-anchor-profile</i> <b>association</b>
<b>Context</b>	show>system>security>tls
<b>Description</b>	This command displays information about server and client profiles that are using the specified TLS trust anchor profile.
<b>Parameters</b>	<i>trust-anchor-profile</i> — Specifies the trust anchor profile, up to 32 characters maximum.
<b>Output</b>	The following output is an example of trust anchor profile information.

### Sample Output

```
*A:Dut-C> show system security tls trust-anchor-profile
=====
Trust Anchor Profile Information
=====
Name                                     CA Profiles Down
-----
tap                                     0
tap-alt1                               0
tap-alt2                               0
tap-empty                              0
=====

*A:Dut-C> show system security tls trust-anchor-profile "tap"
=====
CA-profile List for Trust Anchor "tap"
=====
CA Profile Name                         AdminState      OperState
-----
chainA_l1                              up              up
revChainA_l1                           up              up
=====
*A:Dut-C>show>tls#
```





## 10 Facility Alarms

### 10.1 Facility Alarms Overview

Facility Alarms provide a useful tool for operators to easily track and display the basic status of their equipment facilities. Facility Alarm support is intended to cover a focused subset of router states that are likely to indicate service impacts (or imminent service impacts) related to the overall state of hardware assemblies (cards, fans, links, and so on).

In the CLI, for brevity, the keyword or command **alarm** is used for commands related to Facility Alarms. This chapter may occasionally use the term **alarm** as a short form for **facility alarm**.

The CLI display for `show` routines allows the system operator to easily identify current facility alarm conditions and recently cleared facility alarms without searching event logs or monitoring various card and port show commands to determine the health of basic equipment in the system such as cards and ports.

The SR OS alarm model is based on RFC 3877, *Alarm Management Information Base (MIB)*, (which evolved from the IETF Disman drafts).

---

## 10.2 Facility Alarms vs. Log Events

Facility Alarms are different than log events. Facility Alarms have a state (at least two states: active and clear) and a duration, and can be modeled with state transition events (raised, cleared). A log event occurs when the state of some object in the system changes. Log events notify the operator of a state change (for example, a port going down, an IGP peering session coming up, and so on). Facility alarms show the list of hardware objects that are currently in a bad state. Facility alarms can be examined at any time by an operator, whereas log events can be sent by a router asynchronously when they occur (for example, as an SNMP notification or trap, or a syslog event).

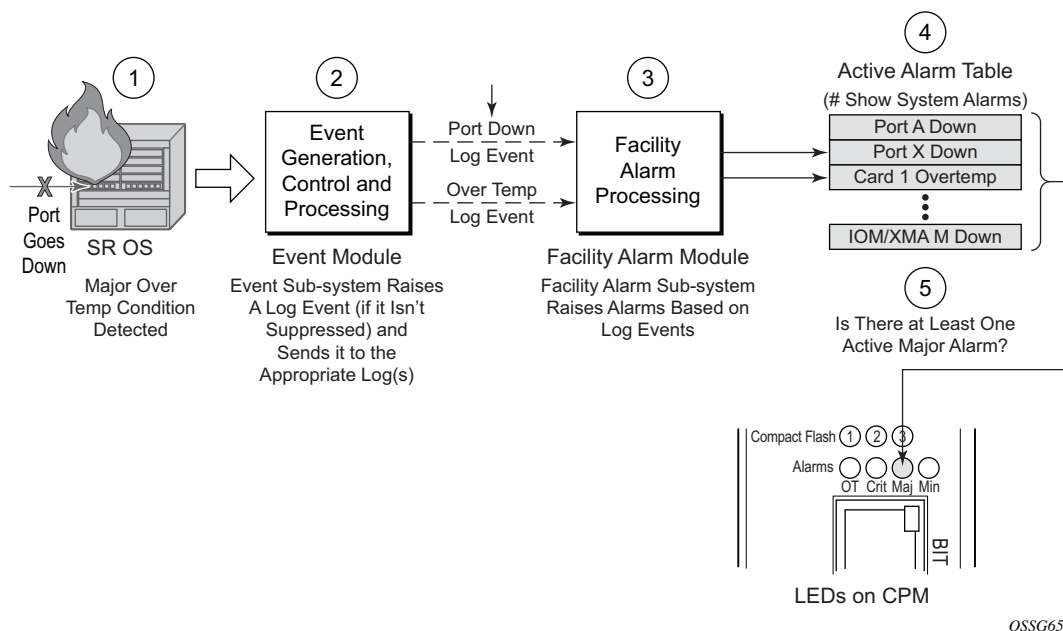
While log events provide notifications about a large number of different types of state changes in SR OS, facility alarms are intended to cover a focused subset of router states that are likely to indicate service impacts (or imminent service impacts) related to the overall state of hardware assemblies (cards, fans, links, and so on).

The facility alarm module processes log events in order to generate the raised and cleared state for the facility alarms. If a raising log event is suppressed under event-control, then the associated facility alarm will not be raised. If a clearing log event is suppressed under event-control, then it is still processed for the purpose of clearing the associated facility alarm. If a log event is a raising event for a Facility Alarm, and the associated Facility Alarm is raised, then changing the log event to **suppress** will clear the associated Facility Alarm.

Log event filtering, throttling and discarding of log events during overload do not affect facility alarm processing. In all cases, non-suppressed log events are processed by the facility alarm module before they are discarded.

[Figure 26](#) illustrates the relationship of log events, facility alarms and the LEDs.

**Figure 26 Log Events, Facility Alarms and LEDs**



Facility Alarms are different and independent functionality from other uses of the term alarm in SR OS such as:

- Log events that use the term **alarm** (tmnxEqPortSonetAlarm)
- **configure card fp hi-bw-mcast-src [alarm]**
- **configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms**
- **configure port ethernet report-alarm**
- **configure system thresholds no memory-use-alarm**
- **configure system thresholds rmon no alarm**
- **configure system security cpu-protection policy alarm**

---

## 10.3 Facility Alarm Severities and Alarm LED Behavior

The Alarm LEDs on the CPM/CCM reflects the current status of the Facility Alarms:

- The Critical Alarm LED is lit if there is 1 or more active Critical Facility Alarms
- Similarly with the Major and Minor alarm LEDs
- The OT Alarm LED is not controlled by the Facility Alarm module

The supported alarm severities are as follows:

- Critical (with an associated LED on the CPM/CCM)
- Major (with an associated LED on the CPM/CCM)
- Minor (with an associated LED on the CPM/CCM)
- Warning (no LED)

Facility alarms inherit their severity from the raising log event.

A raising log event for a facility alarm configured with a severity of *indeterminate* or *cleared* will result in the facility alarm not being raised. But, a clearing log event is processed in order to clear facility alarms, regardless of the severity of the clearing log event.

Changing the severity of a raising log event only affects subsequent occurrences of that log event and facility alarms. Facility alarms that are already raised when their raising log event severity is changed maintain their original severity.

---

## 10.4 Facility Alarm Hierarchy

Facility Alarms for children objects is not raised for failure of a parent object. For example, when an MDA or XMA fails (or is shutdown) there is not a set of port facility alarms raised.

When a parent facility alarm is cleared, children facility alarms that are still in occurrence on the node appears in the active facility alarms list. For example, when a port fails there is a port facility alarm, but if the MDA or XMA is later shutdown the port alarm is cleared (and a card alarm will be active for the MDA or XMA). If the MDA or XMA comes back into service, and the port is still down, then a port alarm becomes active once again.

The supported facility alarm hierarchy is as follows (parent objects that are down cause alarms in all children to be masked):

- CPM -> Compact Flash
- CCM -> Compact Flash
- IOM/IMM -> MDA -> Port -> Channel
- XCM -> XMA -> Port
- MCM -> MDA -> Port -> Channel



**Note:** A masked facility alarm is not the same as a cleared facility alarm. The cleared facility alarm queue does not display entries for previously raised facility alarms that are currently masked. If the masking event goes away, then the previously raised facility alarms will once again be visible in the active facility alarm queue.

## 10.5 Facility Alarm List

Table 119 and Table 120 show the supported Facility Alarms.

**Table 119 Facility Alarm, Facility Alarm Name, Raising Log Event, Sample Details String and Clearing Log Event**

Facility Alarm	Facility Alarm Name/Raising Log Event	Sample Details String	Clearing Log Event
7-2001-1	tmnxEqCardFailure	Class MDA Module: failed, reason: Mda 1 failed startup tests	tmnxChassisNotificationClear
7-2003-1	tmnxEqCardRemoved	Class CPM Module: removed	tmnxEqCardInserted
7-2004-1	tmnxEqWrongCard	Class IOM Module: wrong type inserted	tmnxChassisNotificationClear
7-2005-1	tmnxEnvTempTooHigh	Chassis 1: temperature too high	tmnxChassisNotificationClear
7-2011-1	tmnxEqPowerSupplyRemoved	Power supply 1, power lost	tmnxEqPowerSupplyInserted
7-2017-1	tmnxEqSynclftimingHoldover	Synchronous Timing interface in holdover state	tmnxEqSynclftimingHoldoverClear
7-2019-1	tmnxEqSynclftimingRef1Alarm with attribute tmnxSynclftimingNotifyAlarm == 'los(1)'	Synchronous Timing interface, alarm los on reference 1	tmnxEqSynclftimingRef1AlarmClear
7-2019-2	tmnxEqSynclftimingRef1Alarm with attribute tmnxSynclftimingNotifyAlarm == 'oof(2)'	Synchronous Timing interface, alarm oof on reference 1	same as 7-2019-1
7-2019-3	tmnxEqSynclftimingRef1Alarm with attribute tmnxSynclftimingNotifyAlarm == 'oopir(3)'	Synchronous Timing interface, alarm oopir on reference 1	same as 7-2019-1
7-2021-x	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2	same as 7-2019-x but for ref2
7-2030-x	same as 7-2019-x but for the BITS input	same as 7-2019-x but for the BITS input	same as 7-2019-x but for the BITS input
7-2033-1	tmnxChassisUpgradeInProgress	Class CPM Module: software upgrade in progress	tmnxChassisUpgradeComplete

**Table 119 Facility Alarm, Facility Alarm Name, Raising Log Event, Sample Details String and Clearing Log Event (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Sample Details String	Clearing Log Event
7-2073-x	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input	same as 7-2019-x but for the BITS2 input
7-2092-1	tmnxEqPowerCapacityExceeded	The system has reached maximum power capacity <x> watts	tmnxEqPowerCapacityExceededClear
7-2094-1	tmnxEqPowerLostCapacity	The system can no longer support configured devices. Power capacity dropped to <x> watts	tmnxEqPowerLostCapacityClear
7-2096-1	tmnxEqPowerOverloadState	The system has reached critical power capacity. Increase available power now	tmnxEqPowerOverloadStateClear
7-2138-1	tmnxEqPhysChassPowerSupOvrTmp	Power supply 2 over temperature	tmnxEqPhysChassPowerSupOvrTmpClr
7-2140-1	tmnxEqPhysChassPowerSupAcFail	Power supply 1 AC failure	tmnxEqPhysChassPowerSupAcFailClr
7-2142-1	tmnxEqPhysChassPowerSupDcFail	Power supply 2 DC failure	tmnxEqPhysChassPowerSupDcFailClr
7-2144-1	tmnxEqPhysChassPowerSupInFail	Power supply 1 input failure	tmnxEqPhysChassPowerSupInFailClr
7-2146-1	tmnxEqPhysChassPowerSupOutFail	Power supply 1 output failure	tmnxEqPhysChassPowerSupOutFailClr
7-2148-1	tmnxEqPhysChassisFanFailure	Fan 2 failed	tmnxEqPhysChassisFanFailureClear
7-2161-1	tmnxEqBpEpromFail	The active CPM is no longer able to access any of backplane EPROMs due to a hardware defect	tmnxEqBpEpromFailClear
7-2163-1	tmnxEqBpEpromWarning	The active CPM is no longer to access one backplane EPROM due to a hardware defect but a redundant EPROM is present and accessible.	tmnxEqBpEpromWarningClear
7-4001-1	tmnxInterChassisCommsDown	Control communications disrupted between the Active CPM and the chassis	tmnxInterChassisCommsUp

**Table 119 Facility Alarm, Facility Alarm Name, Raising Log Event, Sample Details String and Clearing Log Event (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Sample Details String	Clearing Log Event
7-4003-1	tmnxCpmlcPortDown	CPM Interconnect Port is not operational. Error code = invalid-connection	tmnxCpmlcPortUp
7-4007-1	tmnxCpmANoLocalIcPort	CPM A can not reach the chassis using its local CPM interconnect ports	tmnxCpmALocalIcPort Avail
7-4008-1	tmnxCpmBNoLocalIcPort	CPM B can not reach the chassis using its local CPM interconnect ports	tmnxCpmBLocalIcPort Avail
7-4017-1	tmnxSfmlcPortDown	SFM interconnect Port is not operational. Error code = invalid-connection to Fabric 10 IcPort 2	tmnxSfmlcPortUp
59-2004-1	linkDown	Interface intf-towards-node-B22 is not operational	linkUp
64-2091-1	tmnxSysLicenseInvalid	Error - <reason> record. <hw> will reboot the chassis <timeRemaining>	None
64-2092-1	tmnxSysLicenseExpiresSoon	The license installed on <hw> expires <timeRemaining>	None



**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2001-1	tmnxEqCardFailure	Generated when one of the cards in a chassis has failed. The card type may be IOM (or XCM), MDA (or XMA), SFM, CCM, CPM, Compact Flash, and so on. The reason is indicated in the details of the log event or alarm, and also available in the tmnxChassisNotifyCard FailureReason attribute included in the SNMP notification.	The effect is dependent on the card that has failed. IOM (or XCM) or MDA (or XMA) failure will cause a loss of service for all services running on that card. A fabric failure can impact traffic to and from all cards. 7750 SR, 7450 ESS — If the IOM/IMM fails then the two associated MDAs for the slot will also go down. 7950 XRS — If one out of two XMA fails in a XCM slot then the XCM will remain up. If only one remaining operational XMA within a XCM slot fails, then the XCM will go into a booting operational state.	Before taking any recovery steps collect a tech-support file, then try resetting (clear) the card. If unsuccessful, try removing and re-inserting the card. If that does not work then replace the card.
7-2003-1	tmnxEqCardRemoved	Generated when a card is removed from the chassis. The card type may be IOM (or XCM), MDA (or XMA), SFM, CCM, CPM, Compact Flash, and so on.	The effect is dependent on the card that has been removed. IOM (or XCM) or MDA (or XMA) removal will cause a loss of service for all services running on that card. A fabric removal can impact traffic to and from all cards.	Before taking any recovery steps collect a tech-support file, then try re-inserting the card. If unsuccessful, replace the card.

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2004-1	tmnxEqWrong Card	Generated when the wrong type of card is inserted into a slot of the chassis. Even though a card may be physically supported by the slot, it may have been administratively configured to allow only certain card types in a particular slot location. The card type may be IOM (or XCM), MDA (or XMA), SFM, CCM, CPM, Compact Flash, and so on.	The effect is dependent on the card that has been incorrectly inserted. Incorrect IOM (or XCM) or MDA (or XMA) insertion will cause a loss of service for all services running on that card.	Insert the correct card into the correct slot, and ensure the slot is configured for the correct type of card.
7-2005-1	tmnxEnvTemp TooHigh	Generated when the temperature sensor reading on an equipment object is greater than its configured threshold.	This could be causing intermittent errors and could also cause permanent damage to components.	Remove or power down the affected cards, or improve the cooling to the node. More powerful fan trays may also be required.
7-2011-1	tmnxEqPower SupplyRemoved	Generated when: <ul style="list-style-type: none"> <li>• one of the power supplies is removed from the chassis</li> <li>• low input voltage is detected. The operating voltage range for the 7750 SR-7/12 and the 7450 ESS-7/12 is -40 to -72 VDC. The alarm is raised if the system detects that the voltage of the power supply has dropped to -42.5 VDC.</li> </ul>	Reduced power can cause intermittent errors and could also cause permanent damage to components.	Re-insert the power supply or raise the input voltage to above -42.5 VDC

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2017-1	tmnxEqSyncIfTimingHoldover	Generated when the synchronous equipment timing subsystem transitions into a holdover state.	Any node-timed ports will have very slow frequency drift limited by the central clock oscillator stability. The oscillator meets the holdover requirements of a Stratum 3 and G.813 Option 1 clock.	Address issues with the central clock input references.
7-2019-1	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'los(1)'	Generated when an alarm condition on the first timing reference is detected. The type of alarm (los, oof, and so on) is indicated in the details of the log event or alarm, and is also available in the tmnxSyncIfTimingNotifyAlarm attribute included in the SNMP notification. The SNMP notification will have the same indices as those of the tmnxCpmCardTable.	Timing reference 1 cannot be used as a source of timing into the central clock.	Address issues with the signal associated with timing reference 1.
7-2019-2	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oof(2)'	The same cause as 7-2019-1.	The same effect as 7-2019-1.	Address issues with the signal associated with timing reference 1.
7-2019-3	tmnxEqSyncIfTimingRef1Alarm with attribute tmnxSyncIfTimingNotifyAlarm == 'oopir(3)'	The same cause as 7-2019-1.	The same effect as 7-2019-1.	Address issues with the signal associated with timing reference 1.
7-2021-x	same as 7-2019-x but for ref2	The same cause as 7-2019-x but for the second timing reference	The same as 7-2019-x but for the second timing reference.	The same as 7-2019-x but for the second timing reference

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2030-x	same as 7-2019-x but for the BITS input	The same cause as 7-2019-x but for the BITS timing reference	The same as 7-2019-x but for the BITS timing reference	The same as 7-2019-x but for the BITS timing reference
7-2033-1	tmnxChassisUpgradelnProgress	The tmnxChassisUpgradelnProgress notification is generated only after a CPM switchover occurs and the new active CPM is running new software, while the IOMs or XCMs are still running old software. This is the start of the upgrade process. The tmnxChassisUpgradelnProgress notification will continue to be generated every 30 minutes while at least one IOM or XCM is still running older software.	A software mismatch between the CPM and IOM or XCM is generally fine for a short duration (during an upgrade) but may not allow for correct long term operation.	Complete the upgrade of all IOMs or XCMs.
7-2073-x	same as 7-2019-x but for the BITS2 input	The same as 7-2019-x but for the BITS 2 timing reference	The same as 7-2019-x but for the BITS 2 timing reference	The same as 7-2019-x but for the BITS 2 timing reference
7-2092-1	tmnxEqPowerCapacityExceeded	Generated when a device needs power to boot, but there is not enough power capacity to support the device.	A non-powered device will not boot until the power capacity is increased to support the device.	Add a new power supply to the system, or change the faulty power supply with a working one.
7-2094-1	tmnxEqPowerLostCapacity	Generated when a power supply fails or is removed which puts the system in an overloaded situation.	Devices are powered off in order of lowest power priority until the available power capacity can support the powered devices.	Add a new power supply to the system, or change the faulty power supply with a working one.

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2096-1	tmnxEqPowerOverloadState	Generated when the overloaded power capacity can not support the power requirements and there are no further devices that can be powered off.	The system runs a risk of experiencing brownouts while the available power capacity does not meet the required power consumption.	Add power capacity or manually shutdown devices until the power capacity meets the power needs.
7-2138-1	tmnxEqPhysChassPowerSupOvrTmp	Generated when the temperature sensor reading on a power supply module is greater than its configured threshold.	This could be causing intermittent errors and could also cause permanent damage to components.	Remove or power down the affected power supply module or improve the cooling to the node. More powerful fan trays may also be required. The power supply itself may be faulty so replacement may be necessary.
7-2140-1	tmnxEqPhysChassPowerSupAcFail	Generated when an AC failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If unsuccessful, replace the power supply.
7-2142-1	tmnxEqPhysChassPowerSupDcFail	Generated when an DC failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If unsuccessful, then replace the power supply.
7-2144-1	tmnxEqPhysChassPowerSupInFail	Generated when an input failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.
7-2146-1	tmnxEqPhysChassPowerSupOutFail,	Generated when an output failure is detected on a power supply.	Reduced power can cause intermittent errors and could also cause permanent damage to components.	First try re-inserting the power supply. If that doesn't work, then replace the power supply.

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-2148-1	tmnxEqPhysChassisFanFailure	Generated when one of the fans in a fan tray has failed.	This could cause the temperature to rise and result in intermittent errors and potentially permanent damage to components.	Replace the fan tray immediately, improve the cooling to the node, or reduce the heat being generated in the node by removing cards or powering down the node.
7-2161-1	tmnxEqBpEepromFail	The tmnxEqBpEepromFail alarm is generated when the active CPM is no longer able to access any of backplane EPROMs due to a hardware defect.	The active CPM is at risk of failing to initialize after node reboot due to not being able to access the BP EPROM to read the chassis type.	The system does not self-recover and Nokia Support has to be contacted for further instructions.
7-2163-1	tmnxEqBpEepromWarning	The tmnxEqBpEepromWarning alarm is generated when the active CPM is no longer able to access one backplane EPROM due to a hardware defect but a redundant EPROM is present and accessible.	There is no effect on system operation.	No recovery action required.
7-4001-1	tmnxInterChassisCommsDown	The tmnxInterChassisCommsDown alarm is generated when the active CPM cannot reach the far-end chassis.	The resources on the far-end chassis are not available. This event for the far-end chassis means that the CPM, SFM, and XCM cards in the far-end chassis will reboot and remain operationally down until communications are re-established.	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-4003-1	tmnxCpmlcPortDown	The tmnxCpmlcPortDown alarm is generated when the CPM interconnect port is not operational. The reason may be a cable connected incorrectly, a disconnected cable, a faulty cable, or a misbehaving CPM interconnect port or card.	At least one of the control plane paths used for inter-chassis CPM communication is not operational. Other paths may be available.	A manual verification and testing of each CPM interconnect port is required to ensure fully functional operation. Physical replacement of cabling may be required.
7-4007-1	tmnxCpmANoLocalIcPort	The tmnxCpmANoLocalIcPort alarm is generated when the CPM cannot reach the other chassis using its local CPM interconnect ports.	<p>Another control communications path may still be available between the CPM and the other chassis via the mate CPM in the same chassis. If that alternative path is not available then complete disruption of control communications to the other chassis will occur and the tmnxInterChassisCommsDown alarm is raised.</p> <p>A tmnxCpmANoLocalIcPort alarm on the active CPM indicates that a further failure of the local CPM interconnect ports on the standby CPM will cause complete disruption of control communications to the other chassis and the tmnxInterChassisCommsDown alarm is raised.</p> <p>A tmnxCpmANoLocalIcPort alarm on the standby CPM indicates that a CPM switchover may cause temporary disruption of control communications to the other chassis while the rebooting CPM comes back into service.</p>	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
7-4008-1	tmnxCpmBNoLocallcPort	The same as 7-4007-1.	The same as 7-4007-1.	The same as 7-4007-1.
7-4009-1	tmnxCpmALocallcPortAvail	The tmnxCpmALocallcPortAvail notification is generated when the CPM re-establishes communication with the other chassis using its local CPM interconnect ports.	A new control communications path is now available between the CPM_A and the other chassis,	
7-4010-1	tmnxCpmBLocallcPortAvail	The same as 7-4009-1.	The same as 7-4009-1.	The same as 7-4009-1.
7-4017-1	tmnxSfmlcPortDown	The tmnxSfmlcPortDown alarm is generated when the SFM interconnect port is not operational. The reason may be a cable connected incorrectly, a disconnected cable, a faulty cable, or a misbehaving SFM interconnect port or SFM card.	This port can no longer be used as part of the user plane fabric between chassis. Other fabric paths may be available resulting in no loss of capacity.	A manual verification and testing of each SFM interconnect port is required to ensure fully functional operation. Physical replacement of cabling may be required.
59-2004-1	linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state).	The indicated interface is taken down.	If the ifAdminStatus is down then the interface state is deliberate and there is no recovery. If the ifAdminStatus is up then try to determine that cause of the interface going down: cable cut, distal end went down, and so on.



**Table 120 Facility Alarm Name/Raising Log Event, Cause, Effect and Recovery (Continued)**

Facility Alarm	Facility Alarm Name/Raising Log Event	Cause	Effect	Recovery
64-2091-1	tmnxSysLicenseInvalid	Generated when the license becomes invalid for the reason specified in the log event/alarm.	The system will reboot at the end of the time remaining.	Configure a valid license file location and file name.
64-2092-1	tmnxSysLicenseExpiresSoon	Generated when the license is due to expire soon.	The system will reboot at the end of the time remaining.	Configure a valid license file location and file name.

The linkDown Facility Alarm is supported for the objects listed in [Table 121](#) (note that all objects may not be supported on all platforms):

**Table 121 linkDown Facility Alarm Support**

Object	Supported
Ethernet Ports	Yes
Sonet Section, Line and Path (POS)	Yes
TDM Ports (E1, T1, DS3) including CES MDAs/CMAs	Yes
TDM Channels (DS3 channel configured in an STM-1 port)	Yes
ATM Ports	Yes
Ethernet LAGs	No
APS groups	No
Bundles (MLPPP, IMA, and so on)	No
ATM channels, Ethernet VLANs, Frame Relay DLCIs	No



---

## 10.6 Configuring Logging with CLI

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

### 10.6.1 Basic Facility Alarm Configuration

The most basic facility alarm configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays an alarm configuration example.

```
A:ALA-12>config>system# alarms
#-----
      no shutdown
      exit
-----
```

### 10.6.2 Common Configuration Tasks

#### 10.6.2.1 Configuring the Maximum Number of Alarms to Clear

The number of alarms to clear can be configured using the command listed below.

Use the following CLI syntax to configure a log file:

**CLI Syntax:**    config>system  
                      alarms  
                      max-cleared max-alarms

The following displays facility alarm configuration example:

```
ALA-12>config>system# alarms
-----
...
max-cleared 100
```

---

exit

...

-----

# 10.7 Facility Alarms Configuration Command Reference

## 10.7.1 Command Hierarchies

- [Facility Alarm Configuration Commands](#)

### 10.7.1.1 Facility Alarm Configuration Commands

```
config
— system
  — alarms
    — max-cleared maximum
    — [no] shutdown
```

## 10.7.2 Command Descriptions

### 10.7.2.1 Generic Commands

#### alarms

<b>Syntax</b>	<b>alarms</b>
<b>Context</b>	config>system
<b>Description</b>	This command enters the context to configure facility alarm parameters. Alarm support is intended to cover a focused subset of router states that are likely to indicate service impacts (or imminent service impacts) related to the overall state of hardware assemblies (cards, fans, links, and so on).

#### max-cleared

<b>Syntax</b>	<b>max-cleared</b> <i>maximum</i>
<b>Context</b>	config>system>alarms

---

<b>Description</b>	This command configures the maximum number of cleared alarms that the system will store and display.
<b>Default</b>	max-cleared 500
<b>Parameters</b>	<i>maximum</i> — Specifies the maximum number of cleared alarms, up to 500.

## shutdown

<b>Syntax</b>	<b>[no] shutdown</b>
<b>Context</b>	config>system>alarms
<b>Description</b>	This command enables or disables the Facility Alarm functionality. When enabled, the Facility Alarm sub-system tracks active and cleared facility alarms and controls the Alarm LEDs on the CPMs/CFMs. When Facility Alarm functionality is enabled, the alarms are viewed using the show system alarms command(s).
<b>Default</b>	no shutdown

# 10.8 Facility Alarms Show Command Reference

## 10.8.1 Command Hierarchies

- [Show Commands](#)

### 10.8.1.1 Show Commands

```
show
  — system
    — alarms [cleared] [count count] [newer-than days] [severity severity-level]
```

## 10.8.2 Command Descriptions

### 10.8.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

#### alarms

<b>Syntax</b>	<b>alarms</b> [cleared] [count <i>count</i> ] [newer-than <i>days</i> ] [ <b>severity</b> <i>severity-level</i> ]
<b>Context</b>	show>system
<b>Description</b>	This command displays facility alarms on the system. Alarm support is intended to cover a focused subset of router states that are likely to indicate service impacts (or imminent service impacts) related to the overall state of hardware assemblies (cards, fans, links, and so on).
<b>Output</b>	The following is an example of alarm fields.  <a href="#">Table 122</a> describes the alarms output fields.

#### Sample Output

**Table 122 Show Facility Alarms Output Fields**

Label	Description
Index	Alarm index number.
Date/Time	Date and time string for the alarm.
Severity	Severity level of the alarm.
Alarm	Alarm identifier.
Resource	Facility associated with the alarm.
Details	Description of the alarm.

A:Dut-A# show system alarms

=====

Alarms [Critical:1 Major:2 Minor:0 Warning:0 Total:3]

=====

Index	Date/Time	Severity	Alarm	Resource
Details				
8	2011/04/01 18:36:43.80	MAJOR	7-2011-1	Power Supply 1
Power supply 1, power lost				
7	2011/04/01 18:35:57.00	MAJOR	7-2005-1	Chassis 1
Chassis 1: temperature too high				
6	2011/04/01 18:35:24.80	CRITICAL	7-2006-1	Fan 1
Fan 1 failed				

=====

#### Cleared alarms table:

A:Dut-A# show system alarms cleared

=====

Cleared Alarms [Size:500 Total:5 (not wrapped)]

=====

Index	Date/Time	Severity	Alarm	Resource
Details				
5	2011/04/01 18:11:55.00	MAJOR	7-2005-1	Chassis 1
Clear Chassis temperature too high alarm				
3	2011/04/01 18:11:54.50	CRITICAL	7-2051-1	Power Supply 1
Clear Power Supply failure				
2	2011/04/01 18:11:54.40	CRITICAL	7-2050-1	Power Supply 1
Clear Power Supply failure				
4	2011/04/01 18:11:54.10	MINOR	7-2004-1	Fan 1
Clear Fan wrong type failure				
1	2011/04/01 18:11:54.00	CRITICAL	7-2007-1	Power Supply 1
Clear Power Supply failure				

=====



## 11 Standards and Protocol Support



**Note:** The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

### Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

### Application Assurance (AA)

3GPP Release 12 (ADC rules over Gx interfaces)

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

### Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000, *Integrated Local Management Interface (ILMI) Version 4.0*

AF-PHY-0086.001, *Inverse Multiplexing for ATM (IMA) Specification Version 1.1*

AF-TM-0121.000, *Traffic Management Specification Version 4.1*

AF-TM-0150.00, *Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR*

GR-1113-CORE, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1*

GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3*

ITU-T I.432.1, *B-ISDN user-network interface - Physical layer specification: General characteristics (02/99)*

ITU-T I.610, *B-ISDN operation and maintenance principles and functions (11/95)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

### Bidirectional Forwarding Detection (BFD)

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

## **Border Gateway Protocol (BGP)**

draft-hares-idr-update-attr-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-flowspec-path-redirect-05, *Flowspec Indirection-id Redirect (localised ID)*

draft-ietf-idr-flowspec-redirect-ip-02, *BGP Flow-Spec Redirect to IP Action*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*

draft-uttaro-idr-bgp-persistence-03, *Support for Long-lived BGP Graceful Restart*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

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 BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

RFC 4486, *Subcodes for BGP Cease Notification Message*  
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 (helper mode)*  
RFC 4760, *Multiprotocol Extensions for BGP-4*  
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, *Autonomous System Confederations for BGP*  
RFC 5291, *Outbound Route Filtering Capability for BGP-4*  
RFC 5396, *Textual Representation of Autonomous System (AS) Numbers (asplain)*  
RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6  
Next Hop*  
RFC 5575, *Dissemination of Flow Specification Rules*  
RFC 5668, *4-Octet AS Specific BGP Extended Community*  
RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4*  
RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*  
RFC 6811, *Prefix Origin Validation*  
RFC 6996, *Autonomous System (AS) Reservation for Private Use*  
RFC 7311, *The Accumulated IGP Metric Attribute for BGP*  
RFC 7607, *Codification of AS 0 Processing*  
RFC 7674, *Clarification of the Flowspec Redirect Extended Community*  
RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE)  
Information Using BGP*  
RFC 7854, *BGP Monitoring Protocol (BMP)*  
RFC 7911, *Advertisement of Multiple Paths in BGP*  
RFC 7999, *BLACKHOLE Community*  
RFC 8092, *BGP Large Communities Attribute*

## **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)*

---

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

## **Ethernet**

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/Y.1342, *Ethernet Linear Protection Switching*

ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

## **Ethernet VPN (EVPN)**

draft-ietf-bess-evpn-ac-df-01, *AC-Influenced Designated Forwarder Election for EVPN*

draft-ietf-bess-evpn-pref-df-01, *Preference-based EVPN DF Election*

draft-ietf-bess-evpn-prefix-advertisement-11, *IP Prefix Advertisement in EVPN*

*draft-ietf-bess-evpn-proxy-arp-nd-04, Operational Aspects of Proxy-ARP/ND in EVPN Networks*  
*draft-ietf-bess-evpn-vpls-seamless-integ-03, (PBB-)EVPN Seamless Integration with (PBB-)VPLS*  
*draft-snr-bess-pbb-evpn-isid-cmacflush-01, PBB-EVPN ISID-based CMAC-Flush*  
*RFC 7432, BGP MPLS-Based Ethernet VPN*  
*RFC 7623, Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*  
*RFC 8214, Virtual Private Wire Service Support in Ethernet VPN*  
*RFC 8317, Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) an Provider Backbone Bridging EVPN (PBB-EVPN)*  
*RFC 8365, A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

## **Frame Relay**

*ANSI T1.617 Annex D, DSS1 - Signalling Specification For Frame Relay Bearer Service*  
*FRF.1.2, PVC User-to-Network Interface (UNI) Implementation Agreement*  
*FRF.12, Frame Relay Fragmentation Implementation Agreement*  
*FRF.16.1, Multilink Frame Relay UNI/NNI Implementation Agreement*  
*FRF.5, Frame Relay/ATM PVC Network Interworking Implementation*  
*FRF2.2, PVC Network-to-Network Interface (NNI) Implementation Agreement*  
*ITU-T Q.933 Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management*

## **Generalized Multiprotocol Label Switching (GMPLS)**

*draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information*  
*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 Generalized Multi-Protocol Label Switching (GMPLS) Recovery*  
*RFC 5063, Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart (helper mode)*

## **gRPC Remote Procedure Calls (gRPC)**

gnmi.proto, *gRPC Network Management Interface (gNMI), version 0.4.0*

*gRPC Network Management Interface (gNMI), Capabilities, Get, Set, Subscribe  
(ONCE, SAMPLE, ON\_CHANGE)*

## **Intermediate System to Intermediate System (IS-IS)**

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002, Second Edition, Nov. 2002, *Intermediate system to  
Intermediate system intra-domain routing information exchange protocol for  
use in conjunction with the protocol for providing the connectionless-mode  
Network Service (ISO 8473)*

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 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*  
RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*  
RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*  
RFC 8202, *IS-IS Multi-Instance* (single topology)

## **Internet Protocol (IP) — Fast Reroute**

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*  
RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*  
RFC 7431, *Multicast-Only Fast Reroute*  
RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

## **Internet Protocol (IP) — General**

draft-grant-tacacs-02, *The TACACS+ Protocol*  
RFC 768, *User Datagram Protocol*  
RFC 793, *Transmission Control Protocol*  
RFC 854, *Telnet Protocol Specifications*  
RFC 1350, *The TFTP Protocol (revision 2)*  
RFC 2347, *TFTP Option Extension*  
RFC 2348, *TFTP Blocksize Option*  
RFC 2349, *TFTP Timeout Interval and Transfer Size Options*  
RFC 2428, *FTP Extensions for IPv6 and NATs*  
RFC 2784, *Generic Routing Encapsulation (GRE)*  
RFC 2890, *Key and Sequence Number Extensions to GRE*  
RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*  
RFC 4251, *The Secure Shell (SSH) Protocol Architecture*  
RFC 4252, *The Secure Shell (SSH) Authentication Protocol* (publickey, password)  
RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*  
RFC 4254, *The Secure Shell (SSH) Connection Protocol*  
RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*  
RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*  
RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer (ECDSA)*  
RFC 5925, *The TCP Authentication Option*  
RFC 5926, *Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)*  
RFC 6398, *IP Router Alert Considerations and Usage (MLD)*

RFC 6528, *Defending against Sequence Number Attacks*

## Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* (version 1)

draft-dolganow-bess-mvpn-expl-track-01, *Explicit Tracking with Wild Card Routes in Multicast VPN*

draft-ietf-bier-mvpn-11, *Multicast VPN Using BIER*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

draft-ietf-mboned-mtrace-v2-17, *Mtrace Version 2: Traceroute Facility for IP Multicast*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* (auto-RP groups)

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (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 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*



RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

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 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

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 VPN (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) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

RFC 7761, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 8279, *Multicast Using Bit Index Explicit Replication (BIER)*

RFC 8296, *Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks (MPLS encapsulation)*

RFC 8401, *Bit Index Explicit Replication (BIER) Support via IS-IS*

## **Internet Protocol (IP) — Version 4**

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)*

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery (router specification)*

---

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*  
RFC 1534, *Interoperation between DHCP and BOOTP*  
RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*  
RFC 1812, *Requirements for IPv4 Routers*  
RFC 1918, *Address Allocation for Private Internets*  
RFC 2003, *IP Encapsulation within IP*  
RFC 2131, *Dynamic Host Configuration Protocol*  
RFC 2132, *DHCP Options and BOOTP Vendor Extensions*  
RFC 2401, *Security Architecture for Internet Protocol*  
RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*  
RFC 3046, *DHCP Relay Agent Information Option (Option 82)*  
RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*  
RFC 4884, *Extended ICMP to Support Multi-Part Messages (ICMPv4 and ICMPv6 Time Exceeded)*

## **Internet Protocol (IP) — Version 6**

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*  
RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*  
RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*  
RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*  
RFC 3587, *IPv6 Global Unicast Address Format*  
RFC 3596, *DNS Extensions to Support IP version 6*  
RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*  
RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*  
RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service 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, *Internet Protocol Version 6 (IPv6) Addressing Architecture*  
RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*  
RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*  
RFC 4862, *IPv6 Stateless Address Autoconfiguration (router functions)*

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*  
RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*  
RFC 5007, *DHCPv6 Leasequery*  
RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*  
RFC 5722, *Handling of Overlapping IPv6 Fragments*  
RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 (IPv6)*  
RFC 5952, *A Recommendation for IPv6 Address Text Representation*  
RFC 6092, *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* (Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters)  
RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*  
RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*  
RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*  
RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*  
RFC 8201, *Path MTU Discovery for IP version 6*

## **Internet Protocol Security (IPsec)**

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*  
draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*  
RFC 2401, *Security Architecture for the Internet Protocol*  
RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*  
RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*  
RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*  
RFC 2406, *IP Encapsulating Security Payload (ESP)*  
RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*  
RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*  
RFC 2409, *The Internet Key Exchange (IKE)*  
RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*  
RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*  
RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*  
RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*  
RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*  
RFC 3947, *Negotiation of NAT-Traversal in the IKE*

---

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*  
RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec ESP*  
RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*  
RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*  
RFC 4301, *Security Architecture for the Internet Protocol*  
RFC 4303, *IP Encapsulating Security Payload*  
RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*  
RFC 4308, *Cryptographic Suites for IPsec*  
RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*  
RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*  
RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*  
RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*  
RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*  
RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*  
RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol*  
RFC 5903, *ECP Groups for IKE and IKEv2*  
RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*  
RFC 6379, *Suite B Cryptographic Suites for IPsec*  
RFC 6380, *Suite B Profile for Internet Protocol Security (IPsec)*  
RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*  
RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*  
RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*  
RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*  
RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*  
RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*  
RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*

---

## Label Distribution Protocol (LDP)

*draft-ietf-mpls-ldp-ip-pw-capability-09, Controlling State Advertisements Of Non-negotiated LDP Applications*  
*draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities*  
*draft-pdutta-mpls-ldp-v2-00, LDP Version 2*  
*draft-pdutta-mpls-mldp-up-redundancy-00, Upstream LSR Redundancy for Multipoint LDP Tunnels*  
*draft-pdutta-mpls-multi-ldp-instance-00, Multiple LDP Instances*  
*draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction*  
*RFC 3037, LDP Applicability*  
*RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (helper mode)*  
*RFC 5036, LDP Specification*  
*RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs)*  
*RFC 5443, LDP IGP Synchronization*  
*RFC 5561, LDP Capabilities*  
*RFC 5919, Signaling LDP Label Advertisement Completion*  
*RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*  
*RFC 6512, Using Multipoint LDP When the Backbone Has No Route to the Root*  
*RFC 6826, Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*  
*RFC 7032, LDP Downstream-on-Demand in Seamless MPLS*  
*RFC 7552, Updates to LDP for IPv6*

## Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

*draft-mammoliti-l2tp-accessline-avp-04, Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*  
*RFC 2661, Layer Two Tunneling Protocol "L2TP"*  
*RFC 2809, Implementation of L2TP Compulsory Tunneling via RADIUS*  
*RFC 3438, Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*  
*RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3)*  
*RFC 4719, Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*  
*RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

## Management

draft-ietf-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6 (IPv6)*

ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*

ianagmplstc-mib, *IANA-GMPLS-TC-MIB*

ianaiftype-mib, *IANAifType-MIB*

ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*

IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*

IEEE8021-PAE-MIB, *IEEE 802.1X MIB*

IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*

LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*

openconfig-bgp.yang version 3.0.1, *BGP Module*

openconfig-bgp-common.yang version 3.0.1, *BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 3.0.1, *BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 3.0.1, *BGP Common Structure Module*

openconfig-bgp-global.yang version 3.0.1, *BGP Global Module*

openconfig-bgp-neighbor.yang version 3.0.1, *BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 3.0.1, *BGP Peer Group Module*

openconfig-bgp-policy.yang version 4.0.1, *BGP Policy Module*

openconfig-if-aggregate.yang version 2.0.0, *Interfaces Aggregated Model*

openconfig-if-ethernet.yang version 2.0.0, *Interfaces Ethernet Model*

openconfig-if-ip.yang version 2.0.0, *Interfaces IP Module*

openconfig-if-ip-ext.yang version 2.0.0, *Interfaces IP Extensions Module*

openconfig-interfaces.yang version 2.0.0, *Interfaces Module*

openconfig-isis.yang version 0.3.0, *IS-IS Module*  
openconfig-isis-lsp.yang version 0.3.0, *IS-IS LSP Module*  
openconfig-isis-routing.yang version 0.3.0, *IS-IS Routing Module*  
openconfig-lacp.yang version 1.1.0, *LACP Module*  
openconfig-lldp.yang version 0.1.0, *LLDP Module*  
openconfig-local-routing.yang version 1.0.1, *Local Routing Module*  
openconfig-network-instance.yang version 0.8.0, *Network Instance Module*  
openconfig-routing-policy.yang version 3.0.0, *Routing Policy Module*  
openconfig-vlan.yang version 2.0.0, *VLAN Module*  
RFC 1157, *A Simple Network Management Protocol (SNMP)*  
RFC 1212, *Concise MIB Definitions*  
RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*  
RFC 1215, *A Convention for Defining Traps for use with the SNMP*  
RFC 1724, *RIP Version 2 MIB Extension*  
RFC 1901, *Introduction to Community-based SNMPv2*  
RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*  
RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*  
RFC 2206, *RSVP Management Information Base using SMIv2*  
RFC 2213, *Integrated Services Management Information Base using SMIv2*  
RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*  
RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*  
RFC 2515, *Definitions of Managed Objects for ATM Management*  
RFC 2570, *SNMP Version 3 Framework*  
RFC 2571, *An Architecture for Describing SNMP Management Frameworks*  
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*  
RFC 2573, *SNMP Applications*  
RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*  
RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*  
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*  
RFC 2579, *Textual Conventions for SMIv2*  
RFC 2580, *Conformance Statements for SMIv2*

---

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3164, *The BSD syslog Protocol*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4)*

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*



RFC 4220, *Traffic Engineering Link Management Information Base*  
RFC 4273, *Definitions of Managed Objects for BGP-4*  
RFC 4292, *IP Forwarding Table MIB*  
RFC 4293, *Management Information Base for the Internet Protocol (IP)*  
RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*  
RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*  
RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms (TLS)*  
RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*  
RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*  
RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*  
RFC 5102, *Information Model for IP Flow Information Export*  
RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2 (TLS client, RSA public key)*  
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*  
RFC 6991, *Common YANG Data Types*  
RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*  
RFC 7950, *The YANG 1.1 Data Modeling Language*  
SFLOW-MIB, *sFlow MIB Version 1.3 (Draft 5)*

## **Multiprotocol Label Switching — Transport Profile (MPLS-TP)**

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 Transport Profile (MPLS-TP) Identifiers*  
RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*  
RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*  
RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*  
RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*  
RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

## **Multiprotocol Label Switching (MPLS)**

draft-ietf-teas-sr-rsvp-coexistence-rec-02, *Recommendations for RSVP-TE and Segment Routing LSP co-existence*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

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*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

## **Network Address Translation (NAT)**

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

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 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7915, *IP/ICMP Translation Algorithm*

## **Network Configuration Protocol (NETCONF)**

RFC 5277, *NETCONF Event Notifications*

RFC 6022, *YANG Module for NETCONF Monitoring*  
RFC 6241, *Network Configuration Protocol (NETCONF)*  
RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*  
RFC 6243, *With-defaults Capability for NETCONF*  
RFC 7895, *YANG Module Library*

## **Open Shortest Path First (OSPF)**

draft-ietf-ospf-ospfv3-lsa-extend-13, *OSPFv3 LSA Extendibility*  
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 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 4552, *Authentication/Confidentiality for OSPFv3*  
RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*  
RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*  
RFC 5185, *OSPF Multi-Area Adjacency*  
RFC 5187, *OSPFv3 Graceful Restart (helper mode)*  
RFC 5243, *OSPF Database Exchange Summary List Optimization*  
RFC 5250, *The OSPF Opaque LSA Option*  
RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*  
RFC 5340, *OSPF for IPv6*  
RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*  
RFC 5838, *Support of Address Families in OSPFv3*  
RFC 6987, *OSPF Stub Router Advertisement*  
RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*  
RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

## OpenFlow

TS-007, *OpenFlow Switch Specification Version 1.3.1* (OpenFlow-hybrid switches)

## Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*

draft-ietf-pce-segment-routing-08, *PCEP Extensions for Segment Routing*

draft-ietf-pce-stateful-pce-14, *PCEP Extensions for Stateful PCE*

RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

## Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

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 2153, *PPP Vendor Extensions*

RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2615, *PPP over SONET/SDH*

RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

RFC 2878, *PPP Bridging Control Protocol (BCP)*

RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*

RFC 5072, *IP Version 6 over PPP*

## Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points (Gx support as it applies to wireline environment (BNG))*

RFC 3588, *Diameter Base Protocol*

RFC 4006, *Diameter Credit-Control Application*

---

## Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS 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*  
MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*  
RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*  
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 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*  
RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*  
RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*  
RFC 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*  
RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over MPLS Networks*  
RFC 4816, *Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*  
RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*  
RFC 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) Operations, Administration, and Maintenance (OAM) Message Mapping*  
RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*  
RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*  
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 Operations, Administration, and Maintenance (OAM) Interworking*

---

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

## **Quality of Service (QoS)**

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2598, *An Expedited Forwarding PHB*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3260, *New Terminology and Clarifications for Diffserv*

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

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

## **Resource Reservation Protocol — Traffic Engineering (RSVP-TE)**

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions (IF\_ID RSVP\_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures)*

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

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 Record Route Object (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 -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

## **Routing Information Protocol (RIP)**

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

## **Segment Routing (SR)**

draft-filsfils-spring-segment-routing-policy-05, *Segment Routing Policy for Traffic Engineering*

draft-francois-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*

draft-gredler-idr-bgp-ls-segment-routing-ext-03, *BGP Link-State extensions for Segment Routing*

draft-ietf-idr-segment-routing-te-policy-02, *Advertising Segment Routing Policies in BGP*

draft-ietf-isis-segment-routing-extensions-04, *IS-IS Extensions for Segment Routing*

*draft-ietf-mpls-spring-lsp-ping-02, Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane*

*draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing*

*draft-ietf-spring-conflict-resolution-05, Segment Routing MPLS Conflict Resolution*

*draft-ietf-spring-segment-routing-ldp-interop-09, Segment Routing interworking with LDP*

## **Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)**

*ANSI T1.105.03, Jitter Network Interfaces*

*ANSI T1.105.06, Physical Layer Specifications*

*ANSI T1.105.09, Network Timing and Synchronization*

*ITU-T G.703, Physical/electrical characteristics of hierarchical digital interfaces*

*ITU-T G.707, Network node interface for the synchronous digital hierarchy (SDH)*

*ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC)*

*ITU-T G.823, The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*

*ITU-T G.824, The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy*

*ITU-T G.825, The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*

*ITU-T G.841, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002*

*ITU-T G.957, Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*

## **Time Division Multiplexing (TDM)**

*ANSI T1.403, DS1 Metallic Interface Specification*

*ANSI T1.404, DS3 Metallic Interface Specification*

## **Timing**

*GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005*

*GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000*



IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions*, issued 09/2008

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*, issued 03/2003

ITU-T G.8261, *Timing and synchronization aspects in packet networks*, issued 04/2008

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC)*, issued 08/2007

ITU-T G.8264, *Distribution of timing information through packet networks*, issued 10/2008

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization*, issued 10/2010

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network*, issued 07/2014

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

## **Two-Way Active Measurement Protocol (TWAMP)**

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP) (server, unauthenticated mode)*

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

## **Virtual Private LAN Service (VPLS)**

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

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)*

---

## Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

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*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550 Appendix A.8, *RTP: A Transport Protocol for Real-Time Applications* (estimating the interarrival jitter)

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

## Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* (S2a roaming based on GPRS)

# Customer Document and Product Support



## Customer Documentation

[Customer Documentation Welcome Page](#)



## Technical Support

[Product Support Portal](#)



## Documentation Feedback

[Customer Documentation Feedback](#)

