



Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 4.0
ROUTER CONFIGURATION GUIDE

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

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

Copyright 2010 Alcatel-Lucent.
All rights reserved.

Disclaimers

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

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

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

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

Table of Contents

Preface	27
Getting Started	31
Alcatel-Lucent 7705 SAR Router Configuration Process	31
Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F	32
IP Router Configuration	35
Configuring IP Router Parameters	36
Interfaces	36
Network Interface	37
System Interface	38
IP Addresses	39
Internet Protocol Versions	39
IPv6 Address Format	40
IPv6 Headers	40
Neighbor Discovery	42
Router ID	42
Autonomous Systems	43
DHCP Relay and DHCPv6 Relay	44
DHCP	44
ICMP and ICMPv6	45
Static Routes, Dynamic Routes, and ECMP	47
IGP-LDP and Static Route-LDP Synchronization	48
Bidirectional Forwarding Detection (BFD)	49
Router Configuration Process Overview	50
Configuration Notes	51
Reference Sources	51
Configuring an IP Router with CLI	53
Router Configuration Overview	54
System Interface	54
Network Interface	55
Basic Configuration	56
Common Configuration Tasks	57
Configuring a System Name	57
Configuring Interfaces	58
Configuring a System Interface	58
Configuring a Network Interface	58
Configuring IPv6 Parameters	59
Configuring Router Advertisement	60
Configuring ECMP	61
Configuring Static Routes	62
Configuring or Deriving a Router ID	63
Configuring an Autonomous System	64
Configuring ICMP and ICMPv6	64
Configuring DHCP	65
Service Management Tasks	67

Table of Contents

Changing the System Name	67
Modifying Interface Parameters	68
Deleting a Logical IP Interface	69
IP Router Command Reference	71
Command Hierarchies	71
Command Descriptions	77
Configuration Commands	78
Show Commands	110
Clear Commands	142
Debug Commands	146
Filter Policies	151
Configuring Filter Policies	152
Network and Service Interface-based Filtering	153
Filter Policy Entries	154
Applying Filter Policies	154
Packet Matching Criteria	155
Ordering Filter Entries	157
Filter Logs	160
Configuration Notes	161
IP Filters	161
IPv6 Filters	162
MAC Filters	162
Filter Logs	163
Reference Sources	163
Configuring Filter Policies with CLI	165
Basic Configuration	166
Common Configuration Tasks	167
Creating an IPv4 or IPv6 Filter Policy	167
IP Filter Policy	167
IP Filter Entry	169
IP Filter Entry Matching Criteria	170
Creating a MAC Filter Policy	172
MAC Filter Policy	172
MAC Filter Entry	173
MAC Entry Matching Criteria	174
Configuring Filter Log Policies	175
Applying IP and MAC Filter Policies	175
Applying Filter Policies to Network Interfaces	177
Apply a Filter Policy to an Interface	177
Filter Management Tasks	178
Renumbering Filter Policy Entries	178
Modifying an IP Filter Policy	180
Modifying a MAC Filter Policy	181
Removing and Deleting a Filter Policy	182
Removing a Filter from an Ingress SAP or Ingress VPLS SDP	182
Removing a Filter from an Egress Ethernet VPLS SAP	183
Removing a Filter from a Network Interface	183
Deleting a Filter	183
Filter Command Reference	185

Command Hierarchies	185
Command Descriptions	190
Configuration Commands	191
Show Commands	216
Clear Commands	234
Monitor Commands	236
Route Policies	239
Configuring Route Policies	240
Routing Policy and MPLS	240
Policy Statements	241
Default Action Behavior	241
Denied IP Prefixes	242
Controlling Route Flapping	242
Regular Expressions	244
BGP and OSPF Route Policy Support	248
BGP Route Policies	249
Readvertised Route Policies	249
When to Use Route Policies	249
Route Policy Configuration Process Overview	250
Configuration Notes	251
Reference Sources	251
Configuring Route Policies with CLI	253
Route Policy Configuration Overview	254
When to Create Routing Policies	254
Default Route Policy Actions	255
Policy Evaluation	256
Damping	260
Basic Route Policy Configuration	261
Configuring Route Policy Components	263
Beginning the Policy Statement	264
Creating a Route Policy	264
Configuring a Default Action	266
Configuring an Entry	267
Configuring an AS Path (policy-option)	269
Configuring a Community List	269
Configuring Damping	270
Configuring a Prefix List	270
Route Policy Configuration Management Tasks	272
Editing Policy Statements and Parameters	272
Deleting an Entry	273
Deleting a Policy Statement	274
Route Policy Command Reference	275
Command Hierarchies	275
Command Descriptions	278
Configuration Commands	279
Show Commands	303
Standards and Protocol Support	309

List of Tables

Getting Started	31
Table 1: Configuration Process	31
Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison	32
IP Router Configuration	35
Table 3: IPv6 Header Field Descriptions	41
Table 4: ICMP Capabilities for IPv4	46
Table 5: ICMPv6 Capabilities for IPv6	46
Table 6: Route Preference Defaults by Route Type	84
Table 7: Show ARP Table Output Fields	111
Table 8: Show Authentication Statistics Output Fields	112
Table 9: Show BFD Interface Output Fields	114
Table 10: Show BFD Session Output Fields	115
Table 11: Show DHCP Statistics Output Fields	116
Table 12: Show DHCPv6 Statistics Output Fields	118
Table 13: Show DHCP Summary Output Fields	119
Table 14: Show DHCPv6 Summary Output Fields	120
Table 15: Show ECMP Settings Output Fields	121
Table 16: Show FIB Output Fields	122
Table 17: Show ICMPv6 Output Fields	123
Table 18: Show ICMPv6 Interface Output Fields	125
Table 19: Show Standard IP Interface Output Fields	127
Table 20: Show Detailed IP Interface Output Fields	128
Table 21: Show Summary IP Interfaces Output Fields	130
Table 22: Show IPv6 Neighbor Output Fields	131
Table 23: Show Standard Route Table Output Fields	133
Table 24: Show Router Advertisement Output Fields	134
Table 25: Show Static ARP Table Output Fields	137
Table 26: Show Static Route Table Output Fields	138
Table 27: Show Router Status Output Fields	140
Table 28: Show Tunnel Table Output Fields	141
Filter Policies	151
Table 29: MAC Match Criteria Exclusivity Rules	162
Table 30: Show Filter Output Fields	217
Table 31: Show Filter Output Fields (Filter ID Specified)	219
Table 32: Show Filter Associations Output Fields	222
Table 33: Show Filter Counters Output Fields	225

List of Tables

Table 34:	Show Filter Log Output Fields	226
Table 35:	Show Filter Log Bindings	227
Table 36:	Show Filter MAC (No Filter- D Specified)	229
Table 37:	Show Filter MAC (Filter ID Specified)	230
Table 38:	Show Filter MAC Associations	232
Table 39:	Show Filter MAC Counters	233
Route Policies		239
Table 40:	Regular Expression Operators	245
Table 41:	AS Path and Community Regular Expression Examples	245
Table 42:	Show Route Policy Output Fields	308

List of Figures

IP Router Configuration	35
Figure 1: IPv6 Header Format	40
Figure 2: IP Router Configuration Flow	50
Filter Policies	151
Figure 3: Creating and Applying Filter Policies	155
Figure 4: Filtering Process Example	159
Route Policies	239
Figure 5: BGP Route Policy Diagram	248
Figure 6: OSPF Route Policy Diagram	248
Figure 7: Route Policy Configuration and Implementation Flow	250
Figure 8: Route Policy Process Example	257
Figure 9: Next Policy Logic Example	258
Figure 10: Next Entry Logic Example	259
Figure 11: Damping Example	260

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
7710 SR	7710 Service Router
7750 SR	7750 Service Router
9500 MPR	9500 Microwave Packet Radio
ABR	available bit rate area border router
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
ADP	automatic discovery protocol
AFI	authority and format identifier
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system

Acronym	Expansion
ASAP	any service, any port
ASBR	autonomous system boundary router
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BGP	border gateway protocol
BITS	building integrated timing supply
BMCA	best master clock algorithm
BMU	<p>broadcast, multicast, and unknown traffic</p> <p>Traffic that is not unicast. Any nature of multipoint traffic:</p> <ul style="list-style-type: none"> • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BOF	boot options file
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSTA	Broadband Service Termination Architecture

Acronym	Expansion
BTS	base transceiver station
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space
CC	control channel continuity check
CCM	continuity check message
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)

Acronym	Expansion
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-TAG	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DDoS	distributed DoS
DES	data encryption standard
DF	do not fragment
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6
DIS	designated intermediate system
DM	delay measurement
DNS	domain name server
DoS	denial of service
dot1p	IEEE 802.1p bits, found in Ethernet or VLAN ingress packet headers and used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPI	deep packet inspection

Acronym	Expansion
DPLL	digital phase locked loop
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DV	delay variation
e911	enhanced 911 service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)
ECMP	equal cost multi-path
EFM	Ethernet in the first mile
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
ELER	egress label edge router
E&M	ear and mouth earth and magneto exchange and multiplexer
Epipe	Ethernet VLL
EPL	Ethernet private line
ERO	explicit route object
ESD	electrostatic discharge
ESMC	Ethernet synchronization message channel
ETE	end-to-end

Acronym	Expansion
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVDO	evolution - data optimized
EVPL	Ethernet virtual private link
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FF	fixed filter
FIB	forwarding information base
FIFO	first in, first out
FNG	fault notification generator
FOM	figure of merit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GFP	generic framing procedure
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HEC	header error control
HMAC	hash message authentication code

Acronym	Expansion
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
HVPLS	hierarchical virtual private line service
IANA	internet assigned numbers authority
IBN	isolated bonding networks
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
IGP	interior gateway protocol
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
IPoATM	IP over ATM
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization

Acronym	Expansion
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSR	label switch router link-state request
LSU	link-state update
LT	linktrace
LTE	line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE

Acronym	Expansion
LTR	linktrace reply
MA	maintenance association
MAC	media access control
MA-ID	maintenance association identifier
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MC-MLPPP	multi-class multilink point-to-point protocol
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDDB	multidrop data bridge
MDL	maintenance data link
ME	maintenance entity
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification
MHF	MIP half function
MIB	management information base
MIP	maintenance association intermediate point

Acronym	Expansion
MIR	minimum information rate
MLPPP	multilink point-to-point protocol
MP	merge point multilink protocol
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPR	see 9500 MPR
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDU	MAC Service Data Unit
MS-PW	multi-segment pseudowire
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
M-VPLS	management virtual private line service
MW	microwave
N·m	newton meter
NBMA	non-broadcast multiple access (network)
NE	network element
NET	network entity title
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface

Acronym	Expansion
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NSAP	network service access point
NSSA	not-so-stubby area
NTP	network time protocol
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier, level 3
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSPF-TE	OSPF-traffic engineering (extensions)
OSS	operations support system
OSSP	Organization Specific Slow Protocol
OTP	one time password
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities
PCP	priority point code
PDU	protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PHB	per-hop behavior

Acronym	Expansion
PHY	physical layer
PID	protocol ID
PIR	peak information rate
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
POP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PRC	primary reference clock
PSN	packet switched network
PSNP	partial sequence number PDU
PTP	precision time protocol performance transparency protocol
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
QL	quality level
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication

Acronym	Expansion
RED	random early discard
RESV	reservation
RIB	routing information base
RJ-45	registered jack 45
RNC	Radio Network Controller
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSHG	residential split horizon group
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
SAA	service assurance agent
SAP	service access point
SAR-8	7705 Service Aggregation Router - 8-slot chassis
SAR-18	7705 Service Aggregation Router - 18-slot chassis
SAR-F	7705 Service Aggregation Router - fixed form-factor chassis
SAToP	structure-agnostic TDM over packet
SCADA	surveillance, control and data acquisition
SCP	secure copy
SD	signal degrade

Acronym	Expansion
SDH	synchronous digital hierarchy
SDI	serial data interface
SDP	service destination point
SE	shared explicit
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first
SPT	shortest path tree
SR	service router (includes 7710 SR, 7750 SR)
SRLG	shared risk link group
SSH	secure shell
SSM	synchronization status messaging
SSU	system synchronization unit
S-TAG	service VLAN tag
STM1	synchronous transport module, level 1
SVC	switched virtual circuit

Acronym	Expansion
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
TDEV	time deviation
TDM	time division multiplexing
TE	traffic engineering
TFTP	trivial file transfer protocol
TLDP	targeted LDP
TLV	type length value
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier
TPMR	two-port MAC relay
TTL	time to live
TTM	tunnel table manager
U-APS	unidirectional automatic protection switching
UBR	unspecified bit rate
UDP	user datagram protocol
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
V.35	V-series Recommendation 35
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier

Acronym	Expansion
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VRF	virtual routing and forwarding table
VSE	vendor-specific extension
VSO	vendor-specific option
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard
WTR	wait to restore

About This Guide

This guide describes logical IP routing interfaces, IP-based filtering, and routing policy support provided by the 7705 Service Aggregation Router and presents configuration and implementation examples.

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

Audience

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

- IP router configuration
- IP-based filters
- routing policy options

List of Technical Publications

The 7705 SAR OS documentation set is composed of the following guides:

- 7705 SAR OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7705 SAR OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7705 SAR OS Interface Configuration Guide
This guide describes card and port provisioning.
- 7705 SAR OS Router Configuration Guide
This guide describes logical IP routing interfaces, IP-based filtering, and routing policies.
- 7705 SAR OS MPLS Guide
This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol for Traffic Engineering (RSVP-TE), and Label Distribution Protocol (LDP).
- 7705 SAR OS Services Guide
This guide describes how to configure service parameters such as service access points (SAPs), service destination points (SDPs), customer information, and user services.
- 7705 SAR OS Quality of Service Guide
This guide describes how to configure Quality of Service (QoS) policy management.
- 7705 SAR OS Routing Protocols Guide
This guide provides an overview of dynamic routing concepts and describes how to configure them.
- 7705 SAR OS OAM and Diagnostics Guide
This guide provides information on Operations, Administration and Maintenance (OAM) tools.

Multiple PDF File Search

You can use Adobe Reader, Release 6.0 or later, to search multiple PDF files for a term. Adobe Reader displays the results in a display panel. The results are grouped by PDF file. You can expand the entry for each file.



Note: The PDF files in which you search must be in the same folder.

To search multiple PDF files for a term:

Step 1. Open Adobe Reader.

Step 2. Choose Edit – Search from the Adobe Reader main menu. The Search panel appears.

Step 3. Enter the term to search for.

Step 4. Select the All PDF Documents in radio button.

Step 5. Choose the folder in which to search using the drop-down menu.

Step 6. Select the following criteria if required:

- Whole words only
- Case-Sensitive
- Include Bookmarks
- Include Comments

Step 7. Click on the Search button.

Adobe Reader displays the search results. You can expand the entries for each file by clicking on the + symbol.

Step 8. Click on a search result to go directly to that location in the selected file.

Technical Support

If you purchased a service agreement for your 7705 SAR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, check this link for instructions to contact Support personnel:

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

Getting Started

In This Chapter

This chapter provides general process flow information to configure routing entities and IP filters.

Alcatel-Lucent 7705 SAR Router Configuration Process

[Table 1](#) lists the tasks necessary to configure logical IP routing interfaces, IP-based filtering, and routing policies.

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

Table 1: Configuration Process

Area	Task	Chapter
Router configuration	Configure router parameters, including router interface and addresses, ARP, and ICMP	IP Router Configuration on page 35
Protocol configuration	Configure IP and MAC filters	Filter Policies on page 151
	Configure routing policies	Route Policies on page 239
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 309

Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F

The 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F run the same operating system software. The main difference between the products is their hardware platforms.

The 7705 SAR-8 is an 8-slot chassis that supports 2 CSMs, a Fan module, and 6 adapter cards. The 7705 SAR-18 chassis has 18 slots; in Release 4.0, it supports 2 CSMs, a Fan module, an Alarm module, and 12 adapter cards.

The 7705 SAR-F chassis has a fixed hardware configuration. The 7705 SAR-F replaces the CSM, Fan module, and the 16-port T1/E1 ASAP Adapter card and 8-port Ethernet Adapter card with an all-in-one unit that provides comparable functional blocks, as detailed in [Table 2](#).

The fixed configuration of the 7705 SAR-F means that provisioning the router at the “card slot” and “type” levels is preset and is not user-configurable. Operators begin configurations at the port level.



Note: Unless stated otherwise, references to the terms “Adapter card” and “CSM” throughout the 7705 SAR OS documentation set include the equivalent functional blocks on the 7705 SAR-F.

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
CSM	Control and switching functions	The control and switching functions include the console and management interfaces, the alarm and fan functions, the synchronization interfaces, system LEDs, and so on.
Fan module	Integrated with the control and switching functions	

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison (Continued)

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
16-port T1/E1 ASAP Adapter card	16 individual T1/E1 ports on the faceplate	<p>The T1/E1 ports on the 7705 SAR-F are equivalent to the T1/E1 ports on the 16-port T1/E1 ASAP Adapter card, version 1, except that the 16 T1/E1 ports on the 7705 SAR-F support multiple synchronization sources to support two timing references. The 16-port T1/E1 ASAP Adapter card, version 2, also supports two timing references.</p> <p>On the 7705 SAR-8 and 7705 SAR-18, the CLI indicates the MDA type for the 16-port T1/E1 ASAP Adapter card as <code>a16-chds1</code> for version 1 and <code>a16-chds1v2</code> for version 2.</p> <p>On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F ports as <code>i16-chds1</code>.</p>
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	<p>The –48 VDC versions of the 7705 SAR-8 support two versions of the 8-port Ethernet Adapter card, with version 2 having additional support for Synchronous Ethernet. The +24 VDC version of the 7705 SAR-8 supports only version 2 of the 8-port Ethernet Adapter card.</p> <p>The 7705 SAR-18 supports only version 2 of the card.</p> <p>The Ethernet ports on the 7705 SAR-F are functionally equivalent to the Ethernet ports on version 2 of the 8-port Ethernet Adapter card and support multiple synchronization sources to support two timing references.</p> <p>On the 7705 SAR-8, the CLI indicates the MDA type for the 8-port Ethernet Adapter card as <code>a8-eth</code> or <code>a8-ethv2</code>. On the 7705 SAR-18, the CLI indicates the MDA type as <code>a8-ethv2</code>. On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F Ethernet ports as <code>i8-eth</code>.</p>
Requires user configuration at card (IOM) and MDA (adapter card) levels	Configuration at card (IOM) and MDA (adapter card) levels is preset and users cannot change these types	

IP Router Configuration

In This Chapter

This chapter provides information about commands required to configure basic router parameters.

Topics in this chapter include:

- [Configuring IP Router Parameters on page 36](#)
 - [Interfaces on page 36](#)
 - [IP Addresses on page 39](#)
 - [Internet Protocol Versions on page 39](#)
 - [Router ID on page 42](#)
 - [Autonomous Systems on page 43](#)
 - [DHCP Relay and DHCPv6 Relay on page 44](#)
 - [ICMP and ICMPv6 on page 45](#)
 - [Static Routes, Dynamic Routes, and ECMP on page 47](#)
 - [IGP-LDP and Static Route-LDP Synchronization on page 48](#)
 - [Bidirectional Forwarding Detection \(BFD\) on page 49](#)
- [Router Configuration Process Overview on page 50](#)
- [Configuration Notes on page 51](#)
- [Configuring an IP Router with CLI on page 53](#)
- [IP Router Command Reference on page 71](#)

Configuring IP Router Parameters

In order to provision services on a 7705 SAR, IP parameters must be configured on the node. Logical IP routing interfaces must be configured to associate entities, such as a port or the system, with IP addresses.

A special type of IP interface is the system interface. Configuration of the system interface is the first step in the provisioning process. When configured, the system IP address can be advertised via peering or signaling protocols.

A system interface must have a unique IP address with a 32-bit subnet mask (for IPv4) or 128-bit prefix length (for IPv6). The system interface is used as the router identifier by higher-level protocols such as OSPF, IS-IS, and BGP, unless overwritten by an explicit router ID.

The following router parameters can be configured:

- [Interfaces](#)
- [IP Addresses](#)
- [Internet Protocol Versions](#)
- [Router ID](#)
- [Autonomous Systems](#)
- [DHCP Relay and DHCPv6 Relay](#)
- [ICMP and ICMPv6](#)
- [Static Routes, Dynamic Routes, and ECMP](#)
- [IGP-LDP and Static Route-LDP Synchronization](#)
- [Bidirectional Forwarding Detection \(BFD\)](#)

Interfaces

The 7705 SAR routers use different types of interfaces for various functions. Interfaces must be configured with parameters such as the address or port. An interface that is assigned to a port is a network interface. The system interface is a logical entity and is not assigned to a physical port.

The 7705 SAR supports IES and VPRN interfaces. IES is used to provide direct forwarding of IP traffic between CE devices and to facilitate the transport of in-band management traffic over ATM links. VPRN provides a Layer 3 virtual private network service to end customers.

Network Interface

A network interface (a logical IP routing interface) can be configured on a network-facing physical or logical port, and is used for connectivity purposes. Each network interface can have only one IP address. The connections are point-to-point; for example, a network port on an Ethernet interface cannot be connected to a LAN but must be connected to a network interface on another router.

Secondary IP address assignment, which is used to connect the same interface to more than one subnet, is not supported.

Network ports are used to transport Ethernet, ATM, and TDM services by means of pseudowires.

IP address assignment is not supported on access (customer-facing) ports except for services such as IES or VPRN.

The 7705 SAR can be used as an LER (label edge router) or LSR (label switch router).

OSPF, IS-IS, and BGP are supported as dynamic routing protocols, and static routes to next-hop addresses are also supported.

Ethernet Ports and Multiple ARP entries

Multiple far-end MAC addresses can be associated with an Ethernet network port on the Ethernet Adapter card. These IP-to-MAC mappings are stored in the ARP table.

With multiple far-end MAC addresses supported in the ARP table, an Ethernet port can work with multiple network devices located in the same LAN segment. The 7705 SAR provides dynamic addressing by the ARP protocol as soon as MAC address resolution is needed for a given IP address. As devices are added to or removed from the network, the router updates the ARP table, adding new dynamic addresses and aging out those that are not in use.

Using the ARP table, the 7705 SAR inserts the appropriate far-end MAC address into the egress packet after the forwarding decision has been made based on the routing tables.

There is no limit to the number of MAC addresses per port or per adapter card. The system limit is 4096 ARP entries (combination of dynamic and static ARP entries), with a limit of 2047 static ARP entries. If a new MAC address that is not already in the ARP table becomes available, at least one MAC address must be flushed from the ARP table with the command `clear>router>arp`.

Dynamic ARP and Static MAC entry

The MAC address of the far end can be learned dynamically or be statically configured.

ARP is the common way to dynamically resolve the MAC address of next-hop IP hosts and is the primary way to resolve IP-to-MAC associations. ARP packets are sent as soon as a MAC address resolution is needed for a given IP address.

Static configuration of MAC addresses for next-hop routers is also supported. Static configuration provides a higher level of security against IP hijacking attacks.



Notes:

- Because timeout is built into dynamic ARP, the MAC address of the remote peer needs to be renewed periodically. The flow of IP traffic resets the timers back to their maximum values. In the case of LDP ECMP, one link could be used for transporting user MPLS (pseudowire) traffic while the LDP session could be transported on another equal cost link. In ECMP for LDP and static LSP cases, it is important to ensure that the remote MAC address is learned and does not expire. Some of the equal cost links might only be transporting MPLS traffic, and in the absence of IP traffic, learned MAC addresses will eventually expire. Configuring static ARP entries or running continuous IP traffic ensures that the remote MAC address is always known. Running BFD for fast detection of Layer 2 faults or running any OAM tools with SAA ensures that the learned MAC addresses do not expire.
- For information on LDPs and static LSPs, refer to the 7705 SAR OS MPLS Guide.

System Interface

The system interface is associated with the node, not a specific interface. It is used during the configuration of the following entities:

- LSP creation (next hop) — when configuring MPLS paths and LSPs
- the addresses on a target router — to set up an LDP, OSPF, or BGP session between neighbors and to configure SDPs (the system interface is the service tunnel endpoint)

The system interface is also referred to as “the” loopback interface. It is used as the router identifier if a router ID has not been explicitly configured. Additional loopback interfaces can be configured; however, the system interface is a special loopback interface.

The system interface is used to preserve connectivity (when alternate routes exist) and to decouple physical connectivity and reachability. If an interface carrying peering traffic fails, and there are alternative links to the same peer system interface, peering could be either unaffected or reestablished over the alternate links. The system interface IP address is also used for MPLS and pseudowire/VLL signaling (via targeted LDP).

IP Addresses

IP addresses are assigned to system interfaces and to network-facing physical or logical ports. The IP addresses are in the form *<ip_address/prefix_length>* or *<ip_address/subnet mask>*. IP version 4 (IPv4) addresses are supported on all interfaces. IP version 6 (IPv6) addresses are supported on access ports (IES only) and network ports (null or dot1q) on the 8-port Ethernet Adapter card, v2, and on the Ethernet ports on the 7705 SAR-F, as well as on the Ethernet management port.

The 7705 SAR supports IPv6 dual stack on Ethernet access ports and on the management port. Dual stack allows both IPv4 and IPv6 to run simultaneously on the interface.

Internet Protocol Versions

The 7705 SAR supports IP version 4 (IPv4 – RFC 791, *Internet Protocol*) and IP version 6 (IPv6 – RFC 2460, *Internet Protocol, Version 6 Specification*). The 7705 SAR can forward IPv6 packets over static routes for network forwarding, IES services, and node management.

IPv6 is a newer version of IP, designed as a successor to IPv4. Some of the differences between IPv4 and IPv6 are:

- expanded addressing capabilities — IPv6 increases the IP address size from 32 bits (IPv4) to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simplified autoconfiguration of addresses
- header format simplification — some IPv4 header fields have been dropped or made optional to reduce the processing cost of packet handling and to limit the bandwidth cost of the IPv6 header
- improved support for extensions and options — changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future
- flow labeling capability — the capability to enable the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service (QoS) or real-time service, was added in IPv6
- authentication and privacy capabilities — extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6

IPv6 Address Format

IPv6 uses a 128-bit address, as opposed to the IPv4 32-bit address. Unlike IPv4 addresses, which use the dotted-decimal format, with each octet assigned a decimal value from 0 to 255, IPv6 addresses use the colon-hexadecimal format X:X:X:X:X:X:X, where each X is a 16-bit section of the 128-bit address. For example:

2001:0DB8:0000:0000:0000:0000:0000:0000

Leading zeros can be omitted from each block in the address. A series of zeros can be replaced with a double colon. For example:

2001:DB8::

The double colon can only be used once in an address.

The IPv6 prefix is the part of the IPv6 address that represents the network identifier. The network identifier appears at the beginning of the IP address. The IPv6 prefix length, which begins with a forward slash (/), shows how many bits of the address make up the network identifier. For example, the address 1080:6809:8086:6502::1/64 means that the first 64 bits of the address represent the network identifier; the remaining 64 bits represent the node identifier.

IPv6 Headers

The IPv6 header format is shown in [Figure 1](#). [Table 3](#) describes the fields.

Figure 1: IPv6 Header Format

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

21169

Table 3: IPv6 Header Field Descriptions

Field	Description
Version	4-bit IP version number (v6)
Traffic Class	8-bit value that enables a source to identify the delivery classification of its packets
Flow Label	<p>20-bit flow label that can be used by a source to label packets for which the source requests special handling by IPv6 routers; for example, non-default QoS or real-time service</p> <p>A flow contains a series of packets that travel between a particular source and particular destination</p>
Payload Length	<p>The length of the payload (16-bit unsigned integer), which is the rest of the packet following the IPv6 header, in octets</p> <p>Any extension headers that are present in the packet are considered to be part of the payload; therefore, the payload always begins immediately after the Destination Address</p>
Next Header	<p>8-bit selector that identifies the type of header immediately following the IPv6 header. The Next Header uses the same values as the IPv4 protocol field for some protocols; for example, the values for TCP and UDP are the same for both IPv4 and IPv6.</p> <p>The Next Header values differ from IPv4 when IPv6 extension headers are identified or when IPv6 unique protocols, such as ICMPv6, are identified.</p>
Hop Limit	8-bit unsigned integer that is decremented by 1 by each node that forwards the packet. If the hop limit is decremented to 0, the packet is discarded and the node sends the ICMPv6 message “Hop Limit Exceeded in transit” back to the sender.
Source Address	128-bit address of the originator of the packet
Destination Address	128-bit address of the intended recipient of the packet

Neighbor Discovery

IPv6 provides autoconfiguration of addresses, where equipment connecting to an IPv6 network can autoconfigure a usable address. There are two types of address autoconfiguration: stateless and stateful. Stateless autoconfiguration requires no manual configuration of hosts, minimal configuration of routers, and no servers. The host generates its own addresses using locally available information and information advertised by routers, such as the 7705 SAR. Stateless autoconfiguration is a feature of the neighbor discovery protocol.

Stateful autoconfiguration involves hosts obtaining interface addresses and/or configuration information from a server. For more information on stateful configuration, see [DHCP Relay](#) and [DHCPv6 Relay](#).

Stateless autoconfiguration uses two neighbor discovery messages: router solicitation and router advertisement. The host sends router solicitation messages to find routers, and the routers send router advertisement messages to indicate their presence. The host sends the router solicitation message to all routers, requesting the IPv6 prefix as well as the IPv6 address of the routers. Each router responds with a router advertisement message indicating their IPv6 prefix and IPv6 address.

Neighbor discovery performs Layer 2 neighbor address resolution similar to ARP in IPv4. In addition, the neighbor discovery protocol performs a neighbor reachability function, where a “stale” neighbor entry is probed for reachability using a unicast neighbor solicitation message. This function ensures that link-layer address changes will be discovered reliably in addition to confirming the presence of the IPv6 neighbor.

Neighbor discovery is implemented within ICMPv6.

Router ID

The router ID is a 32-bit IP address (IPv4) that uniquely identifies the router within an autonomous system (see [Autonomous Systems](#)).

IS-IS and BGP use the router ID as their system ID.

OSPF routers use the router IDs of the neighbor routers to establish adjacencies. Neighbor IDs are learned when Hello packets are received from the neighbor.

Before configuring OSPF parameters, ensure that the router ID is derived by one of the following methods:

- define the value using the `config>router router-id` command
- define the system interface using the `config>router>interface ip-int-name` command (used if the router ID is not specified with the `config>router router-id` command)

A system interface (also referred to as the loopback address) must have an IP address with a 32-bit subnet mask. The system interface is assigned during the primary router configuration process when the interface is created in the logical IP interface context.

- if you do not specify a router ID, the last 4 bytes of the MAC address are used
- the router ID can be derived on the protocol level; for example, BGP

Autonomous Systems

Networks can be grouped into areas. An area is a collection of network segments within an autonomous system (AS) that have been administratively assigned to the same group. An area's topology is concealed from the rest of the AS, which results in a significant reduction in routing traffic.

Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely on information obtained within the area; no routing information obtained from outside the area can be used. This protects intra-area routing from the injection of bad routing information.

Routers that belong to more than one area are called area border routers. All routers in an AS do not have an identical topological database. An area border router has a separate topological database for each area it is connected to. Two routers, which are not area border routers, belonging to the same area, have identical area topological databases.

Autonomous systems share routing information, such as routes to each destination and information about the route or AS path, with other ASs using BGP. Routing tables contain lists of next hops, reachable addresses, and associated path cost metrics to each router. BGP uses the information and path attributes to compile a network topology.



Note: The 7705 SAR supports IBGP only; it does not support EBGP.

DHCP Relay and DHCPv6 Relay

The 7705 SAR provides DHCP/BOOTP Relay agent services and DHCPv6 Relay agent services for DHCP clients. DHCP is used for IPv4 network addresses and DHCPv6 is used for IPv6 network addresses. Both DHCP and DHCPv6 are known as stateful protocols because they use dedicated servers to maintain parameter information.

In the stateful autoconfiguration model, hosts obtain interface addresses and/or configuration information and parameters from a server. The server maintains a database that keeps track of which addresses have been assigned to which hosts.

The 7705 SAR supports DHCP Relay on the base router, and on access IP interfaces associated with IES and VPRN. Each DHCP instance supports up to 8 DHCP servers.

The 7705 SAR supports DHCPv6 Relay on access IP interfaces associated with IES. Each DHCPv6 instance supports up to 8 DHCPv6 servers. For more information on DHCPv6 Relay, refer to the 7705 SAR OS Services Guide, “DHCP Relay”.



Note: The 7705 SAR acts as a relay agent for DHCP and DHCPv6 requests and responses; it does not function as a DHCP or DHCPv6 server.

DHCP

DHCP is a configuration protocol used to communicate network information and configuration parameters from a DHCP server to a DHCP-aware client. DHCP is based on the BOOTP protocol, with additional configuration options and the added capability of allocating dynamic network addresses. DHCP-capable devices are also capable of handling BOOTP messages.

A DHCP client is an IP-capable device (typically a computer or base station) that uses DHCP to obtain configuration parameters such as a network address. A DHCP server is an Internet host or router that returns configuration parameters to DHCP clients. A DHCP/BOOTP Relay agent is a host or router (for example, the 7705 SAR) that passes DHCP messages between clients and servers.

Home computers in a residential high-speed Internet application typically use the DHCP protocol to have their IP address assigned by their Internet service provider.

The DHCP protocol requires the client to transmit a request packet with a destination address of 255.255.255.255 (broadcast) that is processed by the DHCP server. Since IP routers do not forward broadcast packets, the DHCP client and server must reside on the same network segment. However, for various reasons, it is sometimes impractical to have the server and client reside in the same IP network.

When the 7705 SAR is acting as a DHCP Relay agent, it processes these DHCP broadcast packets and relays them to a preconfigured DHCP server. Therefore, DHCP clients and servers do not need to reside on the same network segment.

DHCP Options

DHCP options are codes that the 7705 SAR inserts in packets being forwarded from a DHCP client to a DHCP server. Some options have additional information stored in suboptions.

The 7705 SAR supports the Relay Agent Information Option 82 as specified in RFC 3046. The following suboptions are supported for the base router:

- action
- circuit ID
- copy-82
- remote ID

ICMP and ICMPv6

Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite as defined in RFC 792, *Internet Control Message Protocol*, for IPv4 and RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. The neighbor discovery capability of ICMPv6 is specified in RFC 4861, *Neighbor Discovery for IP Version 6 (IPv6)*.

ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes. The ICMP ping utility for IPv4 and IPv6 and the ICMP traceroute utility for IPv4 are described in the 7705 SAR OS OAM and Diagnostics Guide, “ICMP Diagnostics”.

The 7705 SAR supports the ICMP capabilities described in [Table 4](#).

Table 4: ICMP Capabilities for IPv4

ICMP Message	Description
Address mask reply	Used to reply to an address mask request with an appropriate subnet mask
Time exceeded (TTL expired)	Generated by a router to inform the source of a packet that was discarded due to the time to live (TTL) field reaching zero Used by the traceroute utility to obtain a list of hosts that the packets traversed from source to destination
Destination unreachable	Generated by a router to inform the source host that the destination is unreachable for a specified reason
Echo request/Echo reply	Used by the ping utility to test whether a host is reachable across an IP network and to measure the roundtrip time for packets sent from the local host to a destination node

The 7705 SAR supports the ICMPv6 capabilities described in [Table 5](#).

Table 5: ICMPv6 Capabilities for IPv6

ICMPv6 Message	Description
Destination unreachable	Generated by a router to inform the source host that the destination is unreachable for a specified reason, other than congestion
Packet too big	Generated by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link.
Time exceeded	Generated by a router to inform the source of a packet that was discarded because the hop limit was exceeded in transit
Parameter problem	Generated by a router to inform the source of a packet that the packet was discarded due to a problem with a field in the IPv6 header or extension header that prevented it from processing the packet

Table 5: ICMPv6 Capabilities for IPv6 (Continued)

ICMPv6 Message	Description
Echo request/Echo reply	Used by the ping utility to test whether a host is reachable across an IP network and to measure the roundtrip time for packets sent from the local host to a destination node
Neighbor Discovery ICMPv6 Messages	
Router solicitation	Sent by a host, when an interface is enabled, to request routers to generate router advertisements immediately rather than at their next scheduled time
Router advertisement	Sent by a router to advertise its presence as well as link and Internet parameters, periodically or in response to a router solicitation message
Neighbor solicitation	Sent by a node to determine the link-layer address of a neighbor or to verify that a neighbor is still reachable
Neighbor advertisement	Sent by a node in response to a neighbor solicitation message Nodes can also send unsolicited neighbor advertisements to announce a link-layer address change

Static Routes, Dynamic Routes, and ECMP

Static routes to next-hop addresses are supported on the 7705 SAR. Dynamic routing using the OSPF, IS-IS, or BGP protocols is also supported.

If the 7705 SAR chassis is equipped with two CSMs (Control and Switching modules) for redundancy, non-stop services are supported. Therefore, if the active CSM experiences an activity switch, all static route entries are maintained.

ECMP (Equal-Cost Multipath Protocol) refers to the distribution of packets over two or more outgoing links that share the same routing cost. ECMP provides a fast local reaction to route failures. ECMP is supported on static routes and dynamic (OSPF, IS-IS, and BGP) routes.

As an example, ECMP for LDP can be used to distribute MPLS traffic across the links in order to balance the traffic load. If ECMP for LDP is enabled and there is more than one pseudowire service configured, load balancing will take place on a per-pseudowire basis. ECMP for LDP will load-balance traffic across all equal-cost links on a per-service basis.



Note: The 7705 SAR does not support load balancing of pure IP traffic or pure MPLS traffic over ECMP routes; that is, it does not support FIB ECMP or LFIB ECMP. The 7705 SAR does, however, support VLL ECMP and VPRN transport tunnel ECMP on the LER node.

If multiple routes are learned with an identical preference using the same protocol, the lowest-cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of ECMP in the `config>router` context.

Preferences are set on static routes in the `config>router>static-route` context. Preferences are set on OSPF routes in the `config>router>ospf` context, on IS-IS routes in the `config>router>isis>level` context, and on BGP routes in the `config>router>bgp` context (refer to the 7705 SAR OS Routing Protocols Guide for OSPF, IS-IS, and BGP configuration).

IGP-LDP and Static Route-LDP Synchronization

With LDP, FECs learned from an interface do not necessarily link to that interface state. As long as the router that advertised the label(s) is reachable, the learned labels are stored in the incoming label map (ILM) table.

Although this feature gives LDP a lot of flexibility, it can also cause problems. For example, when an interface comes back up from a failure or from a shutdown state, the static routes bound to that interface are installed immediately. However, the LDP adjacency to the next hop might not be up, which means that the LDP SDP remains down. In this case, the MPLS traffic will be blackholed until the LDP adjacency comes up.

The same issue is also applicable to dynamic routes (OSPF and IS-IS).

To resolve this issue, the LDP synchronization timer enables synchronization of IGP or static routes to the LDP state.

With IGP, when a link is restored after a failure, IGP sets the link cost to infinity and advertises it. The value advertised in OSPF is 0xFFFF (65535). The value advertised in IS-IS regular metric is 0x3F (63) and in IS-IS wide-metric is 0xFFFFFE (16777214).

After IGP advertises the link cost, the LDP hello adjacency is brought up with the neighbor. The LDP synchronization timer is started by IGP from the time the LDP session to the neighbor is up over the interface. This synchronization timer allows time for the label-FEC bindings to be exchanged.

When the LDP synchronization timer expires, the link cost is restored and is readvertised. IGP will announce a new best next-hop and LDP will use it if the label binding for the neighbor's FEC is available.

The above behavior is similar for static routes. If the static route is enabled for `ldp-sync`, the route is not enabled immediately after the interface to the next hop comes up. Routes are suppressed until the LDP adjacency with the neighbor comes up and the synchronization timer expires. The timer does not start until the LDP adjacency with the neighbor node is fully established. For static routes, the `ldp-sync-timer` function requires LDP to use the interface address, not the system address, as its transport address.

Bidirectional Forwarding Detection (BFD)

BFD is a simple protocol for detecting failures in a network. BFD uses a “hello” mechanism that sends control messages periodically to the far end and receives periodic control messages from the far end. BFD is implemented for static routes in asynchronous mode only, meaning that neither end responds to control messages; rather, the messages are sent in the time period configured at each end.

Due to the lightweight nature of BFD, it can detect failures faster than other detection protocols, making it ideal for use in applications such as mobile transport.

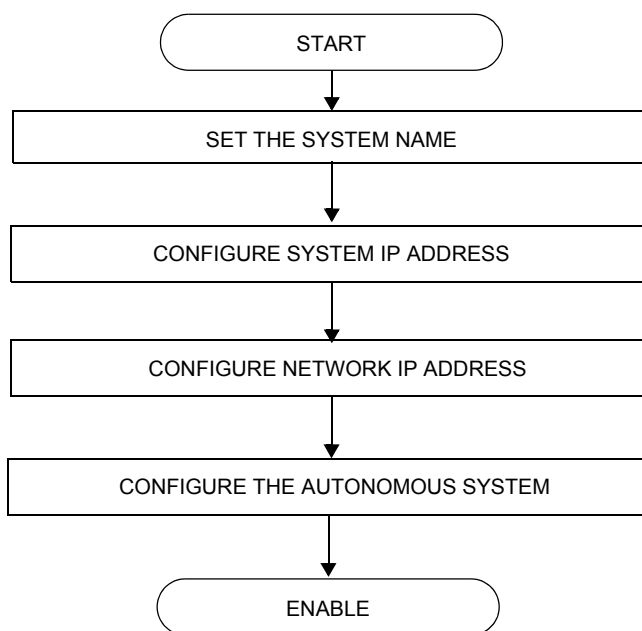
If the configured number of consecutive BFD missed messages is reached, the static route to the peer is declared not active.

BFD is also supported on OSPF, IS-IS, and BGP (refer to the 7705 SAR OS Routing Protocols Guide) and RSVP-TE (refer to the 7705 SAR OS MPLS Guide).

Router Configuration Process Overview

Figure 2 displays the process to configure basic router parameters.

Figure 2: IP Router Configuration Flow



Configuration Notes

The following information describes router configuration caveats.

- A system interface and associated IP address must be specified.
- Boot options file (BOF) parameters must be configured prior to configuring router parameters.

Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to [Standards and Protocol Support](#).

Configuring an IP Router with CLI

This section provides information to configure an IP router.

Topics in this section include:

- [Router Configuration Overview on page 54](#)
 - [System Interface on page 54](#)
 - [Network Interface on page 55](#)
- [Basic Configuration on page 56](#)
- [Common Configuration Tasks on page 57](#)
 - [Configuring a System Name on page 57](#)
 - [Configuring Interfaces on page 58](#)
 - [Configuring IPv6 Parameters on page 59](#)
 - [Configuring Router Advertisement on page 60](#)
 - [Configuring ECMP on page 61](#)
 - [Configuring Static Routes on page 62](#)
 - [Configuring or Deriving a Router ID on page 63](#)
 - [Configuring an Autonomous System on page 64](#)
 - [Configuring ICMP and ICMPv6 on page 64](#)
 - [Configuring DHCP on page 65](#)
- [Service Management Tasks on page 67](#)
 - [Changing the System Name on page 67](#)
 - [Modifying Interface Parameters on page 68](#)
 - [Deleting a Logical IP Interface on page 69](#)

Router Configuration Overview

On a 7705 SAR, an interface is a logical named entity. An interface is created by specifying an interface name under the `config>router` context, the global router configuration context where objects like static routes and dynamic routing are defined. An IP interface name can be up to 32 alphanumeric characters long, must start with a letter, and is case-sensitive; for example, the interface name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed.

To create an interface on an Alcatel-Lucent 7705 SAR, the basic configuration tasks that must be performed are:

- assign a name to the interface
- associate an IP address with the interface
- associate the interface with a network interface or the system interface
- configure appropriate routing protocols

A system interface and network interface should be configured.

System Interface

A system interface is a virtual interface similar to other interfaces but with only some operational parameters. The IP address, shutdown and no shutdown attributes are the only operational parameters for the system interface.

The system interface must have an IP address with a 32-bit subnet mask. The system interface is associated with the node (such as a specific 7705 SAR), not a specific interface. The system interface is also referred to as the loopback interface. The system interface is associated during the configuration of the following entities:

- LSP creation (next hop) — when configuring MPLS paths and LSPs
- the addresses on a target router — to set up an LDP or OSPF session between neighbors and to configure SDPs (the system interface is the service tunnel endpoint)

The system interface is used to preserve connectivity (when alternate routes exist) and to decouple physical connectivity and reachability. If an interface carrying peering traffic fails, and there are alternative routes to the same peer system interface, peering could be either unaffected or re-established over the alternate routes. The system interface IP address is also used for pseudowire/VLL signaling (via targeted LDP).

The system interface is used as the router identifier if a router ID has not been explicitly configured.

Network Interface

A network interface can be configured on a physical or logical port.

Basic Configuration



Note: Refer to [Filter Policies](#) and [Route Policies](#) for information on configuring these policies.

The most basic router configuration must have the following:

- system name
- system address

The following example displays a router configuration.

```
A:ALU-A> config# info
. . .
#-----
# Router Configuration
#-----
    router
        interface "system"
            address 10.10.10.103/32
        exit
        interface "to-104"
            address 10.0.0.103/24
            port 1/1/1
        exit
    exit

#-----
A:ALU-A> config#
```

Common Configuration Tasks

The following sections describe basic system tasks:

- [Configuring a System Name](#)
- [Configuring Interfaces](#)
 - [Configuring a System Interface](#)
 - [Configuring a Network Interface](#)
- [Configuring IPv6 Parameters](#)
- [Configuring Router Advertisement](#)
- [Configuring ECMP](#)
- [Configuring Static Routes](#)
- [Configuring or Deriving a Router ID](#)
- [Configuring an Autonomous System](#)
- [Configuring ICMP and ICMPv6](#)
- [Configuring DHCP](#)

Configuring a System Name

Use the `system` command to configure a name for the device. The name is used in the prompt string. Only one system name can be configured. If multiple system names are configured, the last one configured will overwrite the previous entry.

If special characters are included in the system name string, such as spaces, #, or ?, the entire string must be enclosed within double quotes.

Use the following CLI syntax to configure the system name:

CLI Syntax: `config# system`
 `name system-name`

Example: `config# system`
 `config>system# name ALU-A`
 `ALU-A>config>system# exit all`
 `ALU-A#`

The following example displays the system name output.

```
A:ALU-A>config>system# info
#-----
# System Configuration
#-----
      name "ALU-A"
```

```
location "Kanata, ON, Canada"
snmp
exit
. . .
exit
```

Configuring Interfaces

The following command sequences create a system interface and a logical IP interface. The system interface assigns an IP address to the interface, and then associates the IP interface with a physical port. The logical interface can associate attributes like an IP address or port.

The system interface cannot be deleted.

Configuring a System Interface

Use the following CLI syntax to configure a system interface:

CLI Syntax:

```
config>router
    interface ip-int-name
        address {ip-addr/mask-length}|{ip-addr/netmask}
```

Example:

```
config>router# interface system
config>router>if# address 10.10.10.104/32
config>router>if# exit
```

Configuring a Network Interface

Use the following CLI syntax to configure a network interface:

CLI Syntax:

```
config>router
    interface ip-int-name
        address {ip-addr/mask-length}|{ip-addr/netmask}
        ingress
            filter ip ip-filter-id
        port port-name
```

Example:

```
config>router> interface "to-ALU-2"
config>router>if# address 10.10.24.4/24
config>router>if# port 1/1/1
config>router>if# ingress
config>router>if>ingress# filter ip 10
```

```
config>router>if>ingress# exit
config>router>if# exit
```

The following example displays the IP configuration output showing the interface information.

```
A:ALU-A>config>router# info
#-----
# IP Configuration
#-----
      interface "system"
        address 10.10.0.4/32
      exit
      interface "to-ALU-2"
        address 10.10.24.4/24
        port 1/1/1
        ingress
          filter ip 10
        exit
      exit
...
#-----
A:ALU-A>config>router#
```

Configuring IPv6 Parameters

IP version 6 (IPv6) addresses are supported on access ports (IES only) and network ports (null or dot1q) on the 8-port Ethernet Adapter card, v2, and on the Ethernet ports on the 7705 SAR-F, as well as on the Ethernet management port.

Use the following CLI syntax to configure IPv6 parameters:

CLI Syntax:

```
config>router
  interface ip-int-name
    ipv6
      address ipv6-address/prefix-length [eui-64]
      neighbor ipv6-address mac-address
```

Example:

```
config>router# interface "ipv6-interface"
config>router>if# ipv6
config>router>if>ipv6# address
1080:6809:8086:6502::1/64
```

Configuring Router Advertisement

To configure the router to originate router advertisement messages, the router-advertisement command must be enabled. All other router advertisement configuration parameters are optional. Router advertisement on all IPv6-enabled interfaces will be enabled.

Use the following CLI syntax to enable router advertisement and configure router advertisement parameters:

CLI Syntax:

```
config>router
      router-advertisement
      interface ip-int-name
      current-hop-limit number
      managed-configuration
      max-advertisement-interval seconds
      min-advertisement-interval seconds
      mtu mtu-bytes
      other-stateful-configuration
      prefix ipv6-prefix/prefix-length
      autonomous
      on-link
      preferred-lifetime {seconds | infinite}
      valid-lifetime {seconds | infinite}
      reachable-time milli-seconds
      retransmit-time milli-seconds
      router-lifetime seconds
      no shutdown
```

Example:

```
config>router# router-advertisement
config>router>router-advert# interface "n1"
config>router>router-advert>if# prefix 3::/64
config>router>router-advert>if>prefix# autonomous
config>router>router-advert>if>prefix# on-link
config>router>router-advert>if>prefix# preferred-lifetime
604800
config>router>router-advert>if>prefix# valid-lifetime
2592000
```

The following example displays a router advertisement configuration:

```
A:ALU-A>config>router>router-advert# info
-----
      interface "n1"
      prefix 3::/64
      exit
      no shutdown
-----
A:ALU-A>config>router>router-advert# interface n1
A:ALU-A>config>router>router-advert>if# prefix 3::/64
A:ALU-A>config>router>router-advert>if>prefix# into detail
```

```

-----
autonomous
on-link
preferred-lifetime 604800
valid-lifetime 2592000
-----
A:ALU-A>config>router>router-advert>if>prefix#

```

Configuring ECMP

ECMP (Equal-Cost Multipath Protocol) refers to the distribution of packets over two or more outgoing links that share the same routing cost. ECMP provides a fast local reaction to route failures. ECMP is supported on static routes and dynamic (OSPF, IS-IS, and BGP) routes.

As an example, ECMP for LDP can be used to distribute MPLS traffic across the links in order to balance the traffic load. If ECMP for LDP is enabled and there is more than one pseudowire service configured, load balancing will take place on a per-pseudowire basis. ECMP for LDP will load-balance traffic across all equal-cost links on a per-service basis.



Note: The 7705 SAR does not support load balancing of pure IP traffic or pure MPLS traffic over ECMP routes; that is, it does not support FIB ECMP or LFIB ECMP. The 7705 SAR does, however, support VLL ECMP and VPRN transport tunnel ECMP on the LER node.

If multiple routes are learned with an identical preference using the same protocol, the lowest-cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of ECMP in the `config>router` context.

Use the following CLI syntax to configure ECMP, enable it and specify the maximum number of routes to be used for route sharing (up to 8):

CLI Syntax: `config>router`
 `ecmp max-ecmp-routes`

Example: `config>router# ecmp 7`
 `config>router# exit`

Configuring Static Routes

The 7705 SAR supports both static routes and dynamic routing to next-hop addresses.

For information on configuring OSPF, IS-IS, and BGP routing, refer to the 7705 SAR OS Routing Protocols Guide.

Only one next-hop IP address can be specified per IP interface for static routes.

Use the following CLI syntax to create static route entries:

CLI Syntax:

```
config>router
static-route {ip-prefix/prefix-length} |
{ip-prefix netmask} [preference preference]
[metric metric] [tag tag] [enable | disable]
next-hop {ip-address} [bfd-enable] [ldp-sync]
```

Example:

```
config>router# static-route 192.168.250.0/24 preference 5
metric 1 enable next-hop 10.200.10.3 ldp-sync
config>router# exit
```



Note: If ldp-sync is enabled on a static route, the ldp synchronization timer must also be configured on the associated interface, using the `config>router>interface>ldp-sync-timer` command.

Configuring or Deriving a Router ID

The router ID defaults to the address specified in the system interface command. If the system interface is not configured with an IP address, the router ID inherits the last 4 bytes of the MAC address. Alternatively, the router ID can be explicitly configured with the `config>router>router-id` command.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized, the new router ID is used. To force the new router ID, issue the `shutdown` and `no shutdown` commands for OSPF, IS-IS, or BGP, or restart the entire router.

Use the following CLI syntax to configure a router ID:

CLI Syntax: `config>router`
 `router-id ip-address`
 `interface ip-int-name`
 `address {ip-address/mask | ip-address netmask}`

The following example displays a router ID configuration:

```
A:ALU-B>config>router# info
#-----
# IP Configuration
#-----
      interface "system"
        address 10.10.10.104/32
      exit
      interface "to-103"
        address 10.0.0.104/24
        port 1/1/1
      exit
      router-id 10.10.10.104
...
#-----
A:ALU-B>config>router#
```

Configuring an Autonomous System

Configuring an autonomous system is optional.

Use the following CLI syntax to configure an autonomous system:

CLI Syntax: `config>router`
`autonomous-system as-number`

The following displays an autonomous system configuration example:

```
A:ALU-B>config>router# info
#-----
# IP Configuration
#-----
    interface "system"
        address 10.10.10.103/32
    exit
    interface "to-104"
        address 10.0.0.103/24
        port 1/1/1
    exit
    exit
    autonomous-system 100
    router-id 10.10.10.103
#-----
A:ALU-B>config>router#
```

Configuring ICMP and ICMPv6

Use the following CLI syntax to configure ICMP for the router:

CLI Syntax: `config>router`
`interface ip-int-name`
`icmp`
`mask-reply`
`ttl-expired number seconds`
`unreachables number seconds`

The *number* and *seconds* parameters represent how many of each of these types of ICMP errors the node will generate in the specified interval on the specified interface.

Example: `config>router>if# icmp`
`config>router>if>icmp# mask-reply`
`config>router>if>icmp# ttl-expired 100 20`
`config>router>if>icmp# unreachablees 100 20`

Use the following CLI syntax to configure ICMPv6 for the router:

CLI Syntax:

```
config>router
    interface ip-int-name
        ipv6
            icmp6
                packet-too-big number seconds
                param-problem number seconds
                time-exceeded number seconds
                unreachablees number seconds
```

The *number* and *seconds* parameters represent how many of each of these types of ICMPv6 errors the node will generate in the specified interval on the specified interface.

Example:

```
config>router>if>ipv6# icmp6
config>router>if>ipv6>icmp6# packet-too-big 100 20
config>router>if>ipv6>icmp6# param-problem 100 20
config>router>if>ipv6>icmp6# time-exceeded 100 20
config>router>if>ipv6>icmp6# unreachablees 100 20
```

Configuring DHCP

Use the following CLI syntax to configure DHCP for the router:

CLI Syntax:

```
config>router
    interface interface-name
        dhcp
            description description-string
            option
                action {replace | drop | keep}
                circuit-id [ascii-tuple | port-id | if-name]
                copy-82
                remote-id [mac | string string]
                server server1 [server2...(up to 8 max)]
            no shutdown
        no shutdown
```

Example:

```
A:ALU-41>config>router# interface "DHCP_interface"
A:ALU-41>config>router>if$ dhcp option
A:ALU-41>config>router>if>dhcp>option$ circuit-id ascii-
tuple
A:ALU-41>config>router>if>dhcp>option$ exit
```

The following example displays the router DHCP creation output.

```
A:ALU-41>config>router>if# info detail
-----
...
        dhcp
            shutdown
            no description
            option
                action keep
                circuit-id ascii-tuple
                no remote-id
                no copy-82
            exit
            no server
            no shutdown...
-----
```

Service Management Tasks

This section discusses the following service management tasks:

- [Changing the System Name](#)
- [Modifying Interface Parameters](#)
- [Deleting a Logical IP Interface](#)

Changing the System Name

The `system` command sets the name of the device and is used in the prompt string. Only one system name can be configured. If multiple system names are configured, the last one configured will overwrite the previous entry.

Use the following CLI syntax to change the system name:

CLI Syntax: `config# system`
 name *system-name*

Example: A:ALU-A>config>system# name tgif
 A:TGIF>config>system#

The following example displays the system name change.

```
A:ALU-A>config>system# name TGIF
A:TGIF>config>system# info
#-----
# System Configuration
#-----
      name "TGIF"
      location "Kanata, ON, Canada"
      snmp
        exit
      security
        snmp
          community "private" rwa version both
        exit
      exit
      . . .
-----
A:TGIF>config>system#
```

Modifying Interface Parameters

Starting at the `config>router` level, navigate down to the router interface context.

To modify an IP address, perform the following steps:

Example:

```
A:ALU-A>config>router# interface "to-sr1"
A:ALU-A>config>router>if# shutdown
A:ALU-A>config>router>if# no address
A:ALU-A>config>router>if# address 10.0.0.25/24
A:ALU-A>config>router>if# no shutdown
```

To modify a port, perform the following steps:

Example:

```
A:ALU-A>config>router# interface "to-sr1"
A:ALU-A>config>router>if# shutdown
A:ALU-A>config>router>if# no port
A:ALU-A>config>router>if# port 1/1/2
A:ALU-A>config>router>if# no shutdown
```

The following example displays the interface configuration.

```
A:ALU-A>config>router# info
#-----
# IP Configuration
#-----
    interface "system"
        address 10.0.0.103/32
    exit
    interface "to-sr1"
        address 10.0.0.25/24
        port 1/1/2
    exit
    router-id 10.10.10.104

#-----
A:ALU-A>config>router#
```

Deleting a Logical IP Interface

The `no` form of the `interface` command typically removes the entry, but all entity associations must be shut down and/or deleted before an interface can be deleted.

1. Before an IP interface can be deleted, it must first be administratively disabled with the `shutdown` command.
2. After the interface has been shut down, it can then be deleted with the `no interface` command.

CLI Syntax: `config>router`
`no interface ip-int-name`

Example: `config>router# interface test-interface`
`config>router>if# shutdown`
`config>router>if# exit`
`config>router# no interface test-interface`
`config>router#`

IP Router Command Reference

Command Hierarchies

- [Configuration Commands](#)
 - [Router Commands](#)
 - [Router Interface Commands](#)
 - [Router Interface IPv6 Commands](#)
 - [Router Advertisement Commands](#)
- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)

Configuration Commands

Router Commands

```

config
  — router [router-name]
    — aggregate ip-prefix/ip-prefix-length [summary-only]
    — no aggregate ip-prefix/ip-prefix-length
    — [no] bgp
    — ecmp max-ecmp-routes
    — no ecmp
    — [no] allow-icmp-redirect
    — [no] interface ip-int-name
    — [no] isis
    — [no] ldp
    — [no] mpls
    — [no] ospf
    — [no] policy-options
    — router-id ip-address
    — no router-id
    — rsvp
    — sgt-qos
    — [no] static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference]
      [metric metric] [tag tag] [enable | disable] next-hop ip-address
      [bfd-enable] [ldp-sync]
    — [no] static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference]
      [metric metric] [tag tag] [enable | disable] black-hole
  
```

Router Interface Commands

```

config
  — router [router-name]
    — [no] interface ip-int-name
      — address {ip-address/mask | ip-address netmask}
      — no address
      — [no] allow-directed-broadcasts
      — arp-timeout seconds
      — no arp-timeout
      — bfd transmit-interval [receive receive-interval] [multiplier multiplier]
      — no bfd
      — description description-string
      — no description
      — dhcp
        — description description-string
        — no description
        — [no] option
          — action {replace | drop | keep}
          — no action
          — circuit-id [ascii-tuple | port-id | if-name]
          — no circuit-id
          — [no] copy-82
      
```



```

— remote-id [mac | string string]
— no remote-id
— server server1 [server2...(up to 8 max)]
— no server
— [no] shutdown
— icmp
— [no] mask-reply
— ttl-expired [number seconds]
— no ttl-expired
— unreachableables [number seconds]
— no unreachableables
— ingress
— filter ip ip-filter-id
— filter ipv6 ipv6-filter-id
— no filter [ip ip-filter-id | ipv6 ipv6-filter-id]
— ldp-sync-timer seconds
— no ldp-sync-timer
— [no] loopback
— [no] ntp-broadcast
— port port-name
— no port
— qos network-policy-id
— no qos
— [no] shutdown
— static-arp ip-addr ieee-mac-addr
— no static-arp ip-addr

```

Router Interface IPv6 Commands

```

config
— router [router-name]
— [no] interface ip-int-name
— [no] ipv6
— address ipv6-address/prefix-length [eui-64]
— no address ipv6-address/prefix-length
— icmp6
— packet-too-big [number seconds]
— no packet-too-big
— param-problem [number seconds]
— no param-problem
— time-exceeded [number seconds]
— no time-exceeded
— unreachableables [number seconds]
— no unreachableables
— neighbor ipv6-address mac-address
— no neighbor ipv6-address

```

Router Advertisement Commands

```

config
  — router
    — [no] router-advertisement
      — [no] interface ip-int-name
        — current-hop-limit number
        — no current-hop-limit
        — [no] managed-configuration
        — max-advertisement-interval seconds
        — no max-advertisement-interval
        — min-advertisement-interval seconds
        — no min-advertisement-interval
        — mtu mtu-bytes
        — no mtu
        — [no] other-stateful-configuration
        — prefix ipv6-prefix/prefix-length
        — no prefix
          — [no] autonomous
          — [no] on-link
          — preferred-lifetime {seconds | infinite}
          — no preferred-lifetime
          — valid-lifetime {seconds | infinite}
          — no valid-lifetime
        — reachable-time milli-seconds
        — no reachable-time
        — retransmit-time milli-seconds
        — no retransmit-time
        — router-lifetime seconds
        — no router-lifetime
        — [no] shutdown

```

Show Commands

```

show
  — router router-instance
    — arp [ip-int-name | ip-address/[mask] | mac ieee-mac-address | summary] [arp-type]
    — authentication
      — statistics
      — statistics interface [ip-int-name | ip-address]
      — statistics policy name
    — bfd
      — interface
      — session [src ip-address [dst ip-address] | [detail]]
    — bgp
    — dhcp
      — statistics[interface ip-int-name | ip-address]
      — summary
    — dhcp6
      — statistics[interface ip-int-name | ip-address]
      — summary

```

- **ecmp**
- **fib** *slot-number* [*family*] [*ip-prefix/prefix-length*] [**longer**] [**secondary**]
- **fib** *slot-number* [*family*] **summary**
- **fib** *slot-number* [**nh-table-usage**]
- **icmp6**
 - **interface** *interface-name*
- **interface** [{*ip-address* | *ip-int-name*] [**detail**] [*family*}] | **summary** | **exclude-services**
- **isis**
- **ldp**
- **mpls**
- **neighbor** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-address* | **summary**] [**dynamic** | **static** | **managed**]
- **ospf**
- **policy**
- **route-table** [*family*] [*ip-prefix*[/*prefix-length*] [**longer** | **exact**]] | [**protocol** *protocol-name*] | [**summary**]
- **rsvp**
- **rtr-advertisement** [**interface** *interface-name*] [**prefix** *ipv6-prefix/prefix-length*] [**conflicts**]
- **sgt-qos**
- **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]
- **static-route** [*family*] [*ip-prefix/prefix-length* | **preference** *preference* | **next-hop** *ip-address* | **tag** *tag*] [**detail**]
- **status**
- **tunnel-table** [*ip-address*[/*mask*]] | [**protocol** *protocol* | **sdp** *sdp-id*] [**summary**]

Clear Commands

- clear
 - router
 - **arp** {**all** | *ip-addr* | **interface** {*ip-int-name* | *ip-addr*}}
 - **authentication**
 - **statistics** [**interface** {*ip-int-name* | *ip-address*}]
 - **bfd**
 - **session** **src-ip** *ip-address* **dst-ip** *ip-address*
 - **session** **all**
 - **statistics** **src-ip** *ip-address* **dst-ip** *ip-address*
 - **statistics** **all**
 - **bgp**
 - **dhcp**
 - **statistics** [*ip-int-name* | *ip-address*]
 - **dhcp6**
 - **statistics** [*ip-int-name* | *ip-address*]
 - **icmp6** **all**
 - **icmp6** **global**
 - **icmp6** **interface** *interface-name*
 - **interface** [*ip-int-name* | *ip-addr*] [**icmp**]
 - **isis**
 - **ldp**
 - **mpls**
 - **neighbor** {**all** | *ip-address*}
 - **neighbor** [**interface** *ip-int-name* | *ip-address*]

- ospf
- **router-advertisement** all
- **router-advertisement** [interface *interface-name*]
- rsvp

Debug Commands

- debug
 - trace
 - **destination** *trace-destination*
 - [no] **enable**
 - [no] **trace-point** [module *module-name*] [type *event-type*] [class *event-class*] [task *task-name*] [function *function-name*]
 - **router** *router-instance*
 - [no] **bgp**
 - [no] **ip**
 - [no] **arp**
 - **dhcp** [interface *ip-int-name*]
 - **detail-level** *detail-level* {low| medium | high}
 - no **detail-level**
 - **mode** {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
 - no **mode**
 - [no] **icmp**
 - **icmp6** [ip-int-name]
 - no **icmp6**
 - [no] **interface** [ip-int-name | ip-address]
 - [no] **neighbor**
 - **packet** [ip-int-name | ip-address] [headers] [protocol-id]
 - no **packet** [ip-int-name | ip-address]
 - **route-table** [ip-prefix/prefix-length] [longer]
 - no **route-table**
 - [no] **isis**
 - [no] **ldp**
 - [no] **mpls**
 - [no] **ospf**
 - [no] **rsvp**



Note: For information on MPLS, LDP, and RSVP, see the 7705 SAR OS MPLS Guide. For information on OSPF, IS-IS, and BGP, see the 7705 SAR OS Routing Protocols Guide. For information on self-generated traffic re-marking (sgt-qos), see the 7705 SAR OS Quality of Service Guide. For information on policy options, see [Route Policies](#).

Command Descriptions

- [Configuration Commands on page 78](#)
- [Show Commands on page 110](#)
- [Clear Commands on page 142](#)
- [Debug Commands on page 146](#)

Configuration Commands

- [Generic Commands on page 79](#)
- [Router Global Commands on page 80](#)
- [Router Interface Commands on page 86](#)
- [Router Interface IPv6 Commands on page 94](#)
- [Router Interface DHCP Commands on page 96](#)
- [Router Interface Filter Commands on page 99](#)
- [Router Interface ICMP and ICMPv6 Commands on page 100](#)
- [Router Advertisement Commands on page 104](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>router>interface config>router>if>dhcp
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of the command removes the description string from the context.
Default	no description
Parameters	<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, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>router>interface config>router>if>dhcp config>router>router-advertisement>interface
Description	The shutdown command administratively disables the entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the no shutdown command. Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system-generated configuration files. The no form of the command puts an entity into the administratively enabled state.
Default	no shutdown

Router Global Commands

router

Syntax	router <i>router-name</i>
Context	config
Description	<p>This command enables the context to configure router parameters, interfaces, route policies, and protocols.</p> <p>The router name refers to the router instance (in other commands, the router instance can be either router name or service ID). The 7705 SAR has two routing domains (instances).</p> <p>The base routing domain includes all inband IP traffic; that is, any IP packet arriving at the router over any IP interface (all services, all physical ports on the adapter cards). The routing table for the base instance is populated with these IP addresses.</p> <p>The management routing domain is for out-of-band management traffic; that is, the Mgmt port on the CSM is being used for management traffic. In this case, the routing table for the management routing instance is populated.</p>
Parameters	<i>router-name</i> — the router name
Values	router-name: Base, management
Default	Base

aggregate

Syntax	aggregate <i>ip-prefix/ip-prefix-length</i> [summary-only] no aggregate <i>ip-prefix/ip-prefix-length</i>
Context	config>router
Description	<p>This command creates an aggregate route.</p> <p>Use this command to group a number of routes with common prefixes into a single entry in the routing table. This reduces the number of routes that need to be advertised by this router and reduces the number of routes in the routing tables of downstream routers.</p> <p>Both the original components and the aggregated route (source protocol aggregate) are offered to the Routing Table Manager (RTM). Subsequent policies can be configured to assign protocol-specific characteristics, such as the OSPF tag, to aggregate routes.</p>

Multiple entries with the same prefix but a different mask can be configured; routes are aggregated to the longest mask. If one aggregate is configured as 10.0/16 and another as 10.0.0/24, then route 10.0.128/17 would be aggregated into 10.0/16, and route 10.0.0.128/25 would be aggregated into 10.0.0/24. If multiple entries are made with the same prefix and the same mask, the previous entry is overwritten.

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

Default	no aggregate		
Parameters	<i>ip-prefix/ip-prefix-length</i> — the destination address of the aggregate route in dotted-decimal notation		
	Values	<i>ip-prefix</i>	a.b.c.d (host bits must be 0)
		<i>ip-prefix-length</i>	0 to 32
	summary-only — suppresses advertisement of more specific component routes for the aggregate		
	To remove the summary-only option, enter the same aggregate command without the summary-only parameter.		

ecmp

Syntax	ecmp <i>max-ecmp-routes</i> no ecmp
Context	config>router
Description	This command enables ECMP and configures the number of routes for path sharing; for example, the value 2 means two equal-cost routes will be used for cost sharing.

ECMP (Equal-Cost Multipath Protocol) refers to the distribution of packets over two or more outgoing links that share the same routing cost. ECMP provides a fast local reaction to route failures. ECMP is supported on static routes and dynamic (OSPF, IS-IS, and BGP) routes.

As an example, ECMP for LDP can be used to distribute MPLS traffic across the links in order to balance the traffic load. If ECMP for LDP is enabled and there is more than one pseudowire service configured, load balancing will take place on a per-pseudowire basis. ECMP for LDP will load-balance traffic across all equal-cost links on a per-service basis.



Note: The 7705 SAR does not support load balancing of pure IP traffic or pure MPLS traffic over ECMP routes; that is, it does not support FIB ECMP or LFIB ECMP. The 7705 SAR does, however, support VLL ECMP and VPRN transport tunnel ECMP on the LER node.

If multiple routes are learned with an identical preference using the same protocol, the lowest-cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of ECMP.

ECMP can only be used for routes with the same preference and same protocol. See the [static-route](#) command for information on preferences.

When more ECMP routes are available at the best preference than configured in *max-ecmp-routes*, then the lowest next-hop IP address algorithm is used to select the number of routes configured in *max-ecmp-routes*.

The **no** form of the command disables ECMP path sharing. If ECMP is disabled and multiple routes are available at the best preference and equal cost, the route with the lowest next-hop IP address is used.

The **no** form of the command disables ECMP path sharing.

Default	no ecmp
Parameters	<i>max-ecmp-routes</i> — the maximum number of equal cost routes allowed on this routing table instance, expressed as a decimal integer. Setting ECMP <i>max-ecmp-routes</i> to 1 yields the same result as entering no ecmp .
Values	0 to 8

allow-icmp-redirect

Syntax	[no] allow-icmp-redirect
Context	config>router
Description	This command allows or drops ICMP redirects received on the management interface.

router-id

Syntax	router-id <i>ip-address</i> no router-id
Context	config>router
Description	<p>This command configures the router ID for the router instance.</p> <p>The router ID is used by OSPF and BGP in the routing table manager. IS-IS uses the router ID as its system ID. Refer to the 7705 SAR OS Routing Protocols Guide for information on OSPF, IS-IS, and BGP.</p> <p>When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized, the new router ID is used. This can result in an interim period when different protocols use different router IDs.</p> <p>To force the new router ID to be used, issue the shutdown and no shutdown commands for each protocol that uses the router ID, or restart the entire router.</p>

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

Default The system uses the system interface address (which is also the loopback address).
If a system interface address is not configured, the last 4 bytes of the MAC address are used.

Parameters *ip-address* — the 32-bit router ID expressed in dotted-decimal notation

static-route

Syntax **[no] static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] **next-hop** *ip-address* [**bfd-enable**] [**ldp-sync**]
[no] static-route {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] **black-hole**

Context config>router

Description This command creates IPv4 and IPv6 static route entries for network routes. When configuring a static route, the **next-hop** or **black-hole** parameter must be configured.

The **no** form of the command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, as many parameters as necessary to uniquely identify the static route must be entered.

If the router name is management (see [router](#)), the static routes configured populate the routing table for the management routing instance. Up to 32 IPv4 and 32 IPv6 static routes can be configured for management traffic. This is in addition to the management routes configured using the **bof>static-route** command (refer to the 7705 SAR OS Basic System Configuration Guide, “BOF Command Reference”). The static routes are not added to the routing table until after the configuration file is executed in the application load.

Default **no static-route**

Parameters *ip-prefix/prefix-length* — the destination address of the static route

Values	<i>ipv4-prefix</i>	a.b.c.d (host bits must be 0)
	<i>ipv4-prefix-length</i>	0 to 32

Values	<i>ipv6-prefix</i>	x::x::x::x::x::x (eight 16-bit pieces)
		x::x::x::x::d.d.d.d
		x: [0 to FFFF]H
		d: [0 to 255]D
	<i>ipv6-prefix-length</i>	0 to 128

netmask — the subnet mask in dotted-decimal notation

Values	0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)
---------------	---

preference — the preference of this static route versus the routes from different sources such as OSPF, IS-IS, and BGP, expressed as a decimal integer. When modifying the preference of an existing static route, the metric will not be changed unless specified.

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is according to the route preference defaults listed in [Table 6](#).

Table 6: Route Preference Defaults by Route Type

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes

If multiple routes are learned with an identical preference using the same protocol, the lowest-cost route is used. If multiple routes are learned with an identical preference using the same protocol, and the costs (metrics) are equal, the route to use is determined by the configuration of the [ecmp](#) command.

Default 5

Values 1 to 255

metric — the cost metric for the static route, expressed as a decimal integer. This value is used when importing the static route into other protocols such as OSPF or IS-IS. When the metric is configured as 0, then the metric configured in the other protocol applies.

This value is also used to determine which static route to install in the forwarding table.

- If there are multiple static routes with unequal metrics, the lower-cost (metric) route will be installed.
- If there are multiple static routes with equal metrics, ECMP rules apply.

Default 1

Values 0 to 65535

tag — adds a 32-bit integer tag to the static route. The tag is used in route policies to control distribution of the route into other protocols.

Values 1 to 4294967295

enable — static routes can be administratively enabled or disabled. Use the **enable** parameter to re-enable a disabled static route. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

disable — static routes can be administratively enabled or disabled. Use the **disable** parameter to disable a static route while maintaining the static route in the configuration. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

ip-address — specifies the directly connected next-hop IP address used to reach the destination

The *ip-address* configured here must be on the network side on this node. This address must be associated with a network that is directly connected to a network configured on this node.

Values	<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 to FFFF]H
		d: [0 to 255]D

bfd-enable — associates the state of the static route to a BFD session between the local system and the configured next hop

ldp-sync — prevents the static route from being enabled immediately after the interface to the next hop comes back up after a failure. The static route will be enabled after the LDP adjacency comes up and the LDP synchronization timer expires (see [ldp-sync-timer](#)).

black-hole — specifies that the route is a blackhole route. If the destination address on a packet matches this static route, it will be silently discarded.

The **black-hole** keyword and the **next-hop** keyword are mutually exclusive. If an identical command is entered (with the exception of the **next-hop** parameters), this static route will be replaced with the newly entered configured route, and unless specified, the respective defaults for preference and metric will be applied.

Router Interface Commands

interface

Syntax	[no] interface <i>ip-int-name</i>
Context	config>router
Description	<p>This command creates a logical IP routing interface. When created, attributes like IP address, port, or system can be associated with the IP interface.</p> <p>Interface names are case-sensitive and must be unique within the group of IP interfaces defined for config router interface. Interface names must not be in the dotted-decimal notation of an IP address and must begin with a letter; for example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed.</p> <p>Show commands for router interfaces use either the interface names or the IP addresses. Ambiguity can exist if an IP address is used both as an IP address and an interface name. Duplicate interface names can exist in different router instances, although this is not recommended because it is confusing.</p> <p>When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.</p> <p>Although not a keyword, the interface name “system” is associated with the network entity (such as a specific 7705 SAR), not a specific interface. The system interface is also referred to as the loopback address.</p> <p>The no form of the command removes the IP interface and all the associated configurations. The interface must be administratively shut down before issuing the no interface command.</p>
Default	no interface
Parameters	<p><i>ip-int-name</i> — the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for config router interface commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>Values 1 to 32 characters (must start with a letter)</p> <p>If the <i>ip-int-name</i> already exists, the context is changed to maintain that IP interface. If the <i>ip-int-name</i> already exists as an IP interface defined within the config router commands, an error will occur and the context will not be changed to that IP interface. If the <i>ip-int-name</i> does not exist, the interface is created and the context is changed to that interface for further command processing.</p>

address

Syntax	address <i>{ip-address/mask ip-address netmask}</i> no address
Context	config>router>interface
Description	<p>This command assigns an IP address and IP subnet to an IP interface. Only one IP address can be associated with an IP interface.</p> <p>An IP address must be assigned to each IP interface. An IP address and a mask combine to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.</p> <p>The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted-decimal notation. Show commands display CIDR notation and are stored in configuration files.</p> <p>By default, no IP address or subnet association exists on an IP interface until it is explicitly created.</p> <p>The no form of the command removes the IP address assignment from the IP interface. The no form of this command can only be performed when the IP interface is administratively shut down. Shutting down the IP interface will operationally stop any MPLS LSPs that explicitly reference that IP address. When a new IP address is defined, the IP interface can be administratively enabled (no shutdown), which reinitializes the MPLS LSPs associated with that IP interface.</p> <p>To change an IP address, perform the following steps:</p> <ol style="list-style-type: none"> 1. Shut down the router interface. 2. Assign the new IP address. 3. Enable the router interface. <p>If a new address is entered while another address is still active, the new address will be rejected.</p>
Default	no address
Parameters	<p><i>ip-address</i> — the IP address of the IP interface. The <i>ip-address</i> portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted-decimal notation.</p> <p>Values 1.0.0.0 to 223.255.255.255</p> <p><i>/</i> — the forward slash is a parameter delimiter that separates the <i>ip-address</i> portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the <i>ip-address</i>, the “/” and the <i>mask</i> parameter. If a forward slash does not immediately follow the <i>ip-address</i>, a dotted-decimal mask must follow the prefix.</p>

mask — the subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask* parameter. The *mask* parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address.

Values 1 to 32 (mask length of 32 is reserved for system IP addresses)

netmask — the subnet mask in dotted-decimal notation

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

allow-directed-broadcasts

Syntax [no] **allow-directed-broadcasts**

Context config>router>interface

Description This command enables the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address of another IP interface. The **allow-directed-broadcasts** command on an IP interface enables or disables the transmission of packets destined for the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface is sent as a subnet broadcast out this interface.




Note: Allowing directed broadcasts is a well-known mechanism used for denial-of-service attacks.

By default, directed broadcasts are not allowed and are discarded at this egress IP interface.

The **no** form of the command disables directed broadcasts forwarding out of the IP interface.

Default no **allow-directed broadcasts**

arp-timeout

Syntax	arp-timeout <i>seconds</i> no arp-timeout
Context	config>router>interface
Description	This command configures the minimum interval, in seconds, that an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host. Otherwise, the ARP entry is aged from the ARP table. If the arp-timeout value is set to 0 s, ARP aging is disabled. The no form of the command reverts to the default value.
	Note: The 7705 SAR will attempt to refresh an ARP entry 30 s prior to its expiry. This refresh attempt occurs only if the ARP timeout is set to 45 s or more.
Default	no arp-timeout
Parameters	<i>seconds</i> — the minimum number of seconds a learned ARP entry is stored in the ARP table, expressed as a decimal integer. A value of 0 specifies that the timer is inoperative and learned ARP entries will not be aged. Values 0 to 65535 Default 14400 s (4 h)

bfd

Syntax	bfd <i>transmit-interval</i> [receive <i>receive-interval</i>] [multiplier <i>multiplier</i>] no bfd
Context	config>router>interface
Description	This command configures the time interval in which BFD control messages are transmitted and received on the interface. The <i>multiplier</i> parameter specifies the number of consecutive BFD messages that must be missed by the peer node before the BFD session closes and the upper layer protocols (OSPF, IS-IS, BGP) are notified of the fault.
Default	no bfd
Parameters	<i>transmit-interval</i> — the number of milliseconds between consecutive BFD sent messages Values 100 to 100000 Default 100 <i>receive-interval</i> — the number of milliseconds between consecutive BFD received messages Values 100 to 100000 Default 100

multiplier — the number of consecutive BFD messages that must be missed before the interface is brought down

Values 3 to 20

Default 3

ldp-sync-timer

Syntax	ldp-sync-timer <i>seconds</i> no ldp-sync-timer
Context	config>router>interface
Description	<p>This command configures the IGP-LDP synchronization timer to enable synchronization of IGP and LDP and synchronization of static routes and LDP.</p> <p>When a link is restored after a failure, IGP sets the link cost to infinity and advertises it. The supported IGPs are OSPF and IS-IS. The value advertised in OSPF is 0xFFFF (65535). The value advertised in IS-IS regular metric is 0x3F (63) and in IS-IS wide-metric is 0xFFFFFE (16777214).</p> <p>After IGP advertises the link cost, the LDP hello adjacency is brought up with the neighbor. The LDP synchronization timer is started by IGP from the time the LDP session to the neighbor is up over the interface. This synchronization timer allows time for the label-FEC bindings to be exchanged.</p> <p>When the LDP synchronization timer expires, the link cost is restored and is readvertised. IGP will announce a new best next-hop and LDP will use it if the label binding for the neighbor's FEC is available.</p> <p>The above behavior is similar for static routes. If the static route is enabled for ldp-sync (see static-route), the route is not enabled immediately after the interface to the next hop comes up. Routes are suppressed until the LDP adjacency with the neighbor comes up and the synchronization timer expires. The timer does not start until the LDP adjacency with the neighbor node is fully established. For static routes, the ldp-sync-timer function requires LDP to use the interface address, not the system address, as its transport address.</p> <p>If the user changes the cost of an interface, the new value is advertised at the next flooding of link attributes by IGP. However, if the LDP synchronization timer is still running, the new cost value will only be advertised after the timer expires. Also, if the currently advertised cost is different, the new cost value will be advertised after the user executes any of the following commands:</p> <ul style="list-style-type: none"> • tools>perform>router>ospf>ldp-sync-exit • tools>perform>router>isis>ldp-sync-exit • config>router>interface>no ldp-sync-timer • config>router>ospf>disable-ldp-sync • config>router>isis>disable-ldp-sync <p>Refer to the 7705 SAR OS OAM and Diagnostics Guide for the tools commands and to the 7705 SAR OS Routing Protocols Guide for the OSPF and IS-IS commands.</p>

If the user changes the value of the LDP synchronization timer parameter, the new value will take effect at the next synchronization event. In other words, if the timer is still running, it will continue using the previous value.

If parallel links exist to the same neighbor, the bindings and services should remain up as long as there is one interface that is up. However, the user-configured LDP synchronization timer still applies on the failed then restored interface. In this case, the 7705 SAR will only consider this interface for forwarding after IGP readvertises its actual cost value.

The LDP Sync Timer State is not always synced across to the standby CSM; therefore, after an activity switch, the timer state might not be same as it was on the previously active CSM.

The **no** form of this command disables IGP-LDP synchronization and deletes the configuration.



Note: If the **ldp-sync-timer** value is configured on the interface but LDP is not running on the interface, the configuration will cause the IGP route cost to increase to the maximum value.

Default	no ldp-sync-timer
Parameters	<i>seconds</i> — the time interval for the IGP-LDP synchronization timer
Values	1 to 800

loopback

Syntax	[no] loopback
Context	config>router>interface
Description	This command configures the interface as a loopback interface.
Default	no loopback

ntp-broadcast

Syntax	[no] ntp-broadcast
Context	config>router>interface
Description	<p>This command enables or disables the receiving of SNTP broadcasts on the IP interface.</p> <p>This parameter is only valid when the SNTP broadcast-client global parameter is configured.</p> <p>The no form of the command disables SNTP broadcast received on the IP interface.</p>
Default	no ntp-broadcast

port

Syntax	port port-name no port																		
Context	config>router>interface																		
Description	This command creates an association with a logical IP interface and a physical port.																		
	An interface can also be associated with the system (loopback address).																		
	The command returns an error if the interface is already associated with another port or the system. In this case, the association must be deleted before the command is reattempted.																		
	The port name consists of the <i>port-id</i> (for T1/E1 interfaces and Ethernet interfaces) and an optional encapsulation value (for Ethernet interfaces). The port name can also be the <i>bundle-id</i> used for the multilink bundle associated with the interface. Refer to the 7705 SAR OS Interface Configuration Guide for information on configuring ports.																		
	The no form of the command deletes the association with the port. The no form of this command can only be performed when the interface is administratively down.																		
Default	no port																		
Parameters	port-name — the physical port identifier to associate with the IP interface																		
	Values	<table><tr><td>port-id</td><td colspan="2">slot/mda/port</td></tr><tr><td rowspan="4">bundle-id</td><td>bundle-type-slot/mda.bundle-num</td><td></td></tr><tr><td>bundle</td><td>keyword</td></tr><tr><td>type</td><td>ima, ppp</td></tr><tr><td>bundle-num</td><td>1 to 128</td></tr><tr><td rowspan="2">encap-val</td><td>0 (for null)</td><td></td></tr><tr><td>0 to 4094 (for dot1q)</td><td></td></tr></table>		port-id	slot/mda/port		bundle-id	bundle-type-slot/mda.bundle-num		bundle	keyword	type	ima, ppp	bundle-num	1 to 128	encap-val	0 (for null)		0 to 4094 (for dot1q)
port-id	slot/mda/port																		
bundle-id	bundle-type-slot/mda.bundle-num																		
	bundle	keyword																	
	type	ima, ppp																	
	bundle-num	1 to 128																	
encap-val	0 (for null)																		
	0 to 4094 (for dot1q)																		

qos

Syntax	qos <i>network-policy-id</i> no qos
Context	config>router>interface
Description	<p>This command associates a network Quality of Service (QoS) policy with an IP interface.</p> <p>Only one network QoS policy can be associated with an IP interface at one time. Attempts to associate a second QoS policy return an error.</p> <p>Packets are marked using QoS policies on edge devices. Invoking a QoS policy on a network port allows for the packets that match the policy criteria to be remarked.</p>

The **no** form of the command removes the QoS policy association from the IP interface, and the QoS policy reverts to the default.

Default	qos 1 — IP interface associated with network QoS policy 1
Parameters	<i>network-policy-id</i> — the network policy ID to associate with the IP interface. The policy ID must already exist.
Values	1 to 65535

static-arp

Syntax	static-arp <i>ip-addr</i> <i>ieee-mac-addr</i> no static-arp <i>ip-addr</i>
Context	config>router>interface
Description	<p>This command configures a static ARP entry associating an IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface.</p> <p>If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address is replaced by the new MAC address.</p> <p>A router interface can only have one static ARP entry configured for it. The number of static-arp entries that can be configured on a single node is limited to 8.</p> <p>Static ARP is used when a 7705 SAR needs to know about a device on an interface that cannot or does not respond to ARP requests. Therefore, the 7705 SAR OS configuration can state that if it has a packet that has a certain IP address to send it to the corresponding ARP address.</p> <p>The no form of the command removes a static ARP entry.</p>
Default	no static-arp
Parameters	<p><i>ip-addr</i> — the IP address for the static ARP in IP address dotted-decimal notation</p> <p><i>ieee-mac-addr</i> — the 48-bit MAC address for the static ARP in the form <i>aa:bb:cc:dd:ee:ff</i> or <i>aa-bb-cc-dd-ee-ff</i>, where <i>aa</i>, <i>bb</i>, <i>cc</i>, <i>dd</i>, <i>ee</i> and <i>ff</i> are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.</p>

Router Interface IPv6 Commands

ipv6

Syntax	[no] ipv6
Context	config>router>interface
Description	<p>This command enables the context to configure IPv6 parameters on a router interface. IPv6 parameters can be configured on access ports (IES only) and network ports (null or dot1q) on the 8-port Ethernet Adapter card, v2, and on the Ethernet ports on the 7705 SAR-F, as well as on the Ethernet management port.</p> <p>This command automatically generates an FE80:: link-local address.</p> <p>The no form of the command disables IPv6 on the interface.</p>
Default	no ipv6

address

Syntax	address <i>ipv6-address/prefix-length</i> [eui-64] no address <i>ipv6-address/prefix-length</i>		
Context	config>router>if>ipv6		
Description	This command assigns an IPv6 address to the interface.		
Default	n/a		
Parameters	<i>ipv6-address/prefix-length</i> — the IPv6 address on the interface		
	Values	<i>ipv6-address</i>	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
		<i>prefix-length</i>	1 to 128
	eui-64 — when the eui-64 keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. If a port has not been assigned to the interface, the 64-bit interface identifier is derived from the system MAC address and does not change after a port is added. The same behavior applies for the link-local address.		

neighbor

Syntax	neighbor <i>ipv6-address mac-address</i> no neighbor <i>ipv6-address</i>		
Context	config>router>if>ipv6		
Description	This command configures an IPv6-to-MAC address mapping on the interface. Use this command if a directly attached IPv6 node does not support ICMPv6 neighbor discovery or a static address must be used. This command can only be used on Ethernet interfaces. The <i>ipv6-address</i> must be on the subnet that was configured from the IPv6 address command or a link-local address.		
Parameters	<i>ipv6-address</i> — the IPv6 address on the interface		
Values	<i>ipv6-address</i>	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	
	<i>mac-address</i>	the MAC address for the neighbor in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.	

Router Interface DHCP Commands

dhcp

Syntax	dhcp
Context	config>router>interface
Description	This command enables the context to configure DHCP parameters.

option

Syntax	[no] option
Context	config>router>if>dhcp
Description	<p>This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enters the context for configuring Option 82 suboptions.</p> <p>The no form of this command returns the system to the default.</p>
Default	no option

action

Syntax	action {replace drop keep} no action
Context	config>router>if>dhcp>option
Description	<p>This command configures the processing required when the 7705 SAR receives a DHCP request that already has a Relay Agent Information Option (Option 82) field in the packet.</p> <p>The no form of this command returns the system to the default value.</p>
Default	keep (as per RFC 3046, <i>DHCP Relay Agent Information Option</i> , section 2.1.1, Reforwarded DHCP requests, the default is to keep the existing information intact. The exception to this occurs if the gi-addr (gateway interface address) of the received packet is the same as the ingress address on the router. In this case, the packet is dropped and an error is logged.)
Parameters	<p>replace — in the upstream direction (from the user), the existing Option 82 field is replaced with the Option 82 field from the router. In the downstream direction (towards the user) the Option 82 field is stripped (in accordance with RFC 3046).</p> <p>drop — the packet is dropped, and an error is logged</p>

keep — the existing information is kept in the packet and the router does not add any additional information. In the downstream direction, the Option 82 field is not stripped and is sent on towards the client.

If no Option 82 field is present, the router will not create the Option 82 field.

circuit-id

Syntax	circuit-id [ascii-tuple port-id if-name] no circuit-id
Context	config>router>if>dhcp>option
Description	<p>When enabled, the router sends the interface index (If Index) in the circuit-id suboption of the DHCP packet. The If Index of a router interface can be displayed using the show>router> interface>detail command. This option specifies data that must be unique to the router that is relaying the circuit.</p> <p>If disabled, the circuit-id suboption of the DHCP packet will be left empty.</p> <p>The no form of this command returns the system to the default.</p>
Default	ascii-tuple
Parameters	<p>ascii-tuple — specifies that the ASCII-encoded concatenated “tuple” will be used, where the “tuple” consists of the system name, interface name, and port ID, separated by the syntax symbol “ ”.</p> <p>port-id — specifies that the port identifier will be used. The port identifier can be displayed using the command show>router>interface>detail.</p> <p>if-name — specifies that the interface name will be used</p>

copy-82

Syntax	[no] copy-82
Context	config>router>if>dhcp>option
Description	<p>This command copies the DHCP Option 82 into Option 43 (vendor-specific) on the DHCP offer destined for the DHCP client. This command is used in conjunction with the Auto-Discovery Protocol to allow the Auto-Discovery client node to learn about its network uplink.</p> <p>The no form of this command returns the system to the default.</p>
Default	no copy

remote-id

Syntax	remote-id [mac string <i>string</i>] no remote-id
Context	config>router>if>dhcp>option
Description	<p>When enabled, the router sends the MAC address of the remote end (typically, the DHCP client) in the remote-id suboption of the DHCP packet. This command identifies the host at the other end of the circuit. If disabled, the remote-id suboption of the DHCP packet will be left empty.</p> <p>The no form of this command returns the system to the default.</p>
Default	no remote-id
Parameters	<p>mac — specifies the MAC address of the remote end is encoded in the suboption</p> <p>string <i>string</i> — specifies the remote ID</p> <p>Values up to 32 alphanumeric characters</p>

server

Syntax	server <i>server1</i> [<i>server2</i> ...(up to 8 max)] no server
Context	config>router>if>dhcp
Description	<p>This command specifies a list of servers where requests will be forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP Relay to work. If there are multiple servers specified, then the request is forwarded to all of the servers in the list. There can be a maximum of eight DHCP servers configured.</p>
Default	no server
Parameters	<i>server</i> — specifies the DHCP server IP address

Router Interface Filter Commands

ingress

Syntax	ingress
Context	config>router>interface
Description	<p>This command enables access to the context to configure ingress network filter policies for the IP interface.</p> <p>If an ingress filter is not defined, no filtering is performed.</p>

filter

Syntax	filter ip <i>ip-filter-id</i> filter ipv6 <i>ipv6-filter-id</i> no filter [ip <i>ip-filter-id</i> ipv6 <i>ipv6-filter-id</i>]
Context	config>router>if>ingress
Description	<p>This command associates an IP filter policy with an IPv4 or IPv6 interface.</p> <p>Filter policies control packet forwarding and dropping based on IP match criteria.</p> <p>The <i>ip-filter-id</i> or <i>ipv6-filter-id</i> must have been preconfigured before this filter command is executed. If the filter ID does not exist, an error occurs.</p> <p>Only one filter ID can be specified.</p> <p>The no form of the command removes the filter policy associated with the IP interface.</p>
Default	n/a
Parameters	<p><i>ip-filter-id</i> — the ID for the IPv4 filter policy expressed as a decimal integer. The filter policy must already exist within the config>filter>ip-filter context.</p> <p>Values 1 to 65535</p> <p><i>ipv6-filter-id</i> — the ID for the IPv6 filter policy expressed as a decimal integer. The filter policy must already exist within the config>filter>ip-filter context.</p> <p>Values 1 to 65535</p>



Note: For information on configuring IP filter IDs, see [Creating an IPv4 or IPv6 Filter Policy](#).

Router Interface ICMP and ICMPv6 Commands

icmp

Syntax	icmp
Context	config>router>interface
Description	This command enables access to the context to configure Internet Control Message Protocol (ICMP) parameters on a network IP interface. ICMP is a message control and error reporting protocol that also provides information relevant to IP packet processing.

mask-reply

Syntax	[no] mask-reply
Context	config>router>if>icmp
Description	<p>This command enables or disables responses to ICMP mask requests on the router interface.</p> <p>If a local node sends an ICMP mask request to the router interface, the mask-reply command configures the router interface to reply to the request.</p> <p>The no form of the command disables replies to ICMP mask requests on the router interface.</p>
Default	mask-reply — replies to ICMP mask requests

ttl-expired

Syntax	ttl-expired [<i>number seconds</i>] no ttl-expired
Context	config>router>if>icmp
Description	<p>This command enables the generation of ICMP Time To Live (TTL) expired messages and configures the rate that the messages are issued by the IP interface.</p> <p>By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10-s time interval.</p> <p>The no form of the command disables the generation of TTL expired messages.</p>
Default	ttl-expired 100 10 — maximum of 100 TTL expired message in 10 s

Parameters	<i>number</i> — the maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. The <i>seconds</i> parameter must also be specified.
Values	10 to 100
	<i>seconds</i> — the interval, in seconds, used to limit the number of ICMP TTL expired messages that can be issued, expressed as a decimal integer
Values	1 to 60

unreachables

Syntax	unreachables [<i>number seconds</i>] no unreachables
Context	config>router>if>icmp
Description	<p>This command enables the generation of ICMP host and network destination unreachable messages on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional <i>number</i> and <i>seconds</i> parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.</p> <p>By default, generation of ICMP destination unreachables messages is enabled at a maximum rate of 100 per 10-s time interval.</p> <p>The no form of the command disables the generation of ICMP destination unreachables on the router interface.</p>
Default	unreachables 100 10 — maximum of 100 unreachable messages in 10 s
Parameters	<p><i>number</i> — the maximum number of ICMP unreachable messages to send, expressed as a decimal integer. The <i>seconds</i> parameter must also be specified.</p> <p>Values 10 to 100</p> <p><i>seconds</i> — the interval, in seconds, used to limit the <i>number</i> of ICMP unreachable messages that can be issued, expressed as a decimal integer</p> <p>Values 1 to 60</p>

icmp6

Syntax	icmp6
Context	config>router>if>ipv6
Description	This command enables the context to configure ICMPv6 parameters on an interface.

packet-too-big

Syntax	packet-too-big [<i>number seconds</i>] no packet-too-big
Context	config>router>if>ipv6>icmp6
Description	<p>This command enables the generation of ICMPv6 packet-too-big messages and configures the rate that the messages are issued by the IP interface.</p> <p>The no form of the command disables the sending of ICMPv6 packet-too-big messages.</p>
Default	100 10
Parameters	<p><i>number</i> — the maximum number of packet-too-big messages to send, expressed as a decimal integer, in the time frame specified by the <i>seconds</i> parameter</p> <p>Values 10 to 1000</p> <p><i>seconds</i> — the time frame, in seconds, used to limit the number of packet-too-big messages that can be issued, expressed as a decimal integer</p> <p>Values 1 to 60</p>

param-problem

Syntax	param-problem [<i>number seconds</i>] no param-problem
Context	config>router>if>ipv6>icmp6
Description	<p>This command enables the generation of ICMPv6 param-problem messages and configures the rate that the messages are issued by the IP interface.</p> <p>The no form of the command disables the sending of ICMPv6 param-problem messages.</p>
Default	100 10
Parameters	<p><i>number</i> — the maximum number of param-problem messages to send, expressed as a decimal integer, in the time frame specified by the <i>seconds</i> parameter</p> <p>Values 10 to 1000</p> <p><i>seconds</i> — the time frame, in seconds, used to limit the number of param-problem messages that can be issued, expressed as a decimal integer</p> <p>Values 1 to 60</p>

time-exceeded

Syntax	time-exceeded [<i>number seconds</i>] no time-exceeded
Context	config>router>if>ipv6>icmp6
Description	<p>This command enables the generation of ICMPv6 time-exceeded messages and configures the rate that the messages are issued by the IP interface.</p> <p>The no form of the command disables the sending of ICMPv6 time-exceeded messages.</p>
Default	100 10
Parameters	<p><i>number</i> — the maximum number of time-exceeded messages to send, expressed as a decimal integer, in the time frame specified by the <i>seconds</i> parameter</p> <p>Values 10 to 1000</p> <p><i>seconds</i> — the time frame, in seconds, used to limit the number of time-exceeded messages that can be issued, expressed as a decimal integer</p> <p>Values 1 to 60</p>

unreachables

Syntax	unreachables [<i>number seconds</i>] no unreachables
Context	config>router>if>ipv6>icmp6
Description	<p>This command enables the generation of ICMPv6 host and network destination unreachable messages on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional <i>number</i> and <i>seconds</i> parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.</p> <p>The no form of the command disables the generation of ICMPv6 destination unreachables on the router interface.</p>
Default	100 10
Parameters	<p><i>number</i> — the maximum number of destination unreachable messages to send, expressed as a decimal integer, in the time frame specified by the <i>seconds</i> parameter</p> <p>Values 10 to 1000</p> <p><i>seconds</i> — the time frame, in seconds, used to limit the number of destination unreachable messages that can be issued, expressed as a decimal integer</p> <p>Values 1 to 60</p>

Router Advertisement Commands

router-advertisement

Syntax	[no] router-advertisement
Context	config>router
Description	<p>This command enables the context to configure router advertisement properties. By default, it is disabled for all IPv6-enabled interfaces.</p> <p>The no form of the command disables router advertisement on all IPv6 interfaces.</p>
Default	no router-advertisement

interface

Syntax	[no] interface <i>ip-int-name</i>
Context	config>router>router-advertisement
Description	<p>This command configures router advertisement properties on a specified interface. The interface name must already exist in the config>router>interface context.</p> <p>The no form of the command disables router advertisement on the specified router interface.</p>
Default	n/a
Parameters	<p><i>ip-int-name</i> — the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for config router interface commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>Values 1 to 32 characters (must start with a letter)</p>

current-hop-limit

Syntax	current-hop-limit <i>number</i> no current-hop-limit
Context	config>router>router-advertisement>interface
Description	This command configures the current hop limit in the router advertisement messages. It informs the nodes on the subnet about the hop limit when originating IPv6 packets.
Default	64

Parameters *number* — the hop limit

Values 0 to 255 (a value of 0 means that there are an unspecified number of hops)

managed-configuration

Syntax [no] managed-configuration

Context config>router>router-advertisement>interface

Description This command sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address autoconfigured using stateless address autoconfiguration. Refer to RFC 3315, *Dynamic Host Configuration Protocol (DHCP) for IPv6*.

Default no managed-configuration

max-advertisement-interval

Syntax max-advertisement-interval *seconds*
no max-advertisement-interval

Context config>router>router-advertisement>interface

Description This command configures the maximum interval between sending router advertisement messages.

Default 600

Parameters *seconds* — the maximum interval, in seconds, between sending router advertisement messages

Values 4 to 1800

min-advertisement-interval

Syntax min-advertisement-interval *seconds*
no min-advertisement-interval

Context config>router>router-advertisement>interface

Description This command configures the minimum interval between sending ICMPv6 router advertisement messages.

Default 200

Parameters *seconds* — the minimum interval, in seconds, between sending ICMPv6 router advertisement messages

Values 3 to 1350

mtu

Syntax	mtu <i>mtu-bytes</i> no mtu
Context	config>router>router-advertisement>interface
Description	<p>This command configures the MTU for the nodes to use when sending packets on the link.</p> <p>The no form of the command means that the MTU option is not sent in the router advertisement messages.</p>
Default	no mtu
Parameters	<i>mtu-bytes</i> — the MTU for the nodes to use when sending packets
Values	1280 to 9212

other-stateful-configuration

Syntax	[no] other-stateful-configuration
Context	config>router>router-advertisement>interface
Description	<p>This command sets the “Other configuration” flag. This flag indicates that DHCPv6lite is available for autoconfiguration of other (non-address) information such as DNS-related information or information on other servers in the network. See RFC 3736, <i>Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6</i>.</p>
Default	no other-stateful configuration

prefix

Syntax	prefix <i>ipv6-prefix/prefix-length</i> no prefix
Context	config>router>router-advertisement>interface
Description	<p>This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until it is explicitly configured using prefix statements.</p>
Default	n/a

Parameters	<i>ipv6-prefix/prefix-length</i> — the IPv6 prefix		
	Values	<i>ipv6-prefix</i>	x::x::x::x::x::x (eight 16-bit pieces) x::x::x::x::d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
		<i>prefix-length</i>	4 to 127

autonomous

Syntax	[no] autonomous
Context	config>router>router-advertisement>if>prefix
Description	This command specifies whether the prefix can be used for stateless address autoconfiguration.
Default	autonomous

on-link

Syntax	[no] on-link
Context	config>router>router-advertisement>if>prefix
Description	This command specifies whether the prefix can be used for onlink determination.
Default	on-link

preferred-lifetime

Syntax	preferred-lifetime [<i>seconds</i> infinite] no preferred-lifetime
Context	config>router>router-advertisement>if>prefix
Description	This command configures the remaining time, in seconds, that this prefix will continue to be preferred (time until deprecation). The address generated from a deprecated prefix should not be used as a source address in new communications. However, packets received on such an interface are processed as expected.
Default	604800
Parameters	<i>seconds</i> — the remaining length of time, in seconds, that this prefix will be preferred
	Values 1 to 4294967294
	infinite — the prefix will always be preferred. A value of 4294967295 represents infinity.

valid-lifetime

Syntax	valid-lifetime [<i>seconds</i> infinite] no valid-lifetime
Context	config>router>router-advertisement>if>prefix
Description	This command specifies the length of time, in seconds, that the prefix is valid for the purpose of onlink determination. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.
Default	2592000
Parameters	<i>seconds</i> — the remaining length of time, in seconds, that this prefix will be valid Values 1 to 4294967294 infinite — the prefix will always be valid. A value of 4294967295 represents infinity.

reachable-time

Syntax	reachable-time <i>milli-seconds</i> no reachable-time
Context	config>router>router-advertisement>interface
Description	This command configures how long the router should be considered reachable by other nodes on the link after receiving a reachability confirmation.
Default	no reachable-time
Parameters	<i>milli-seconds</i> — the length of time that the router should be considered reachable Values 0 to 3600000

retransmit-time

Syntax	retransmit-time <i>milli-seconds</i> no retransmit-time
Context	config>router>router-advertisement>interface
Description	This command configures the retransmission frequency of neighbor solicitation messages.
Default	no retransmit-time
Parameters	<i>milli-seconds</i> — the amount of time that a host should wait before retransmitting neighbor solicitation messages Values 0 to 1800000

router-lifetime

Syntax	router-lifetime <i>seconds</i> no router-lifetime
Context	config>router>router-advertisement>interface
Description	This command configures the router lifetime.
Default	no router-lifetime
Parameters	<i>seconds</i> — the length of time, in seconds (relative to the time that the packet is sent), that the prefix is valid for route determination Values 0, 4 to 9000 (a value of 0 means that the router is not a default router on this link)

Show Commands

arp

Syntax `arp [ip-int-name | ip-address/[mask] | mac ieee-mac-address | summary] [arp-type]`

Context show>router

Description This command displays the router ARP table sorted by IP address.

If no command line options are specified, all ARP entries are displayed.



Note: Multiple MAC addresses can be associated with an interface that is a network port.

Parameters

- ip-int-name* — only displays the ARP entry associated with the specified IP interface name
- ip-address/[mask]* — only displays the ARP entry associated with the specified IP address and optional mask
- ieee-mac-addr* — only displays the ARP entry associated with the specified MAC address
- summary** — displays an abbreviated list of ARP entries
- arp-type* — only displays ARP information associated with the specified keyword

Values local, dynamic, static, managed

Output The following output is an example of the ARP table, and [Table 7](#) describes the fields.

Sample Output

```
*A:ALU-A# show router arp
=====
ARP Table
=====
IP Address      MAC Address      Expiry           Type Interface
-----
10.10.0.3       04:5d:ff:00:00:00 00:00:00        Oth  system
10.10.13.1      04:5b:01:01:00:02 03:53:09        Sta  to-ser1
10.10.13.3      04:5d:01:01:00:02 00:00:00        Oth  to-ser1
10.10.34.3      04:5d:01:01:00:01 00:00:00        Oth  to-ser4
10.10.34.4      04:5e:01:01:00:01 01:08:00        Sta  to-ser4
10.10.35.3      04:5d:01:01:00:03 00:00:00        Oth  to-ser5
10.10.35.5      04:5f:01:01:00:03 02:47:07        Sta  to-ser5
192.168.2.93    00:03:47:97:68:7d 00:00:00        Oth  management
=====
No. of ARP Entries: 8
=====
*A:ALU-A#
```

```

*A:ALU-A# show router arp 10.10.0.3
=====
ARP Table
=====
IP Address      MAC Address      Expiry      Type Interface
-----
10.10.0.3       04:5d:ff:00:00:00 00:00:00    Oth  system
=====
*A:ALU-A#

*A:ALU-A# show router arp to-ser1
=====
ARP Table
=====
IP Address      MAC Address      Expiry      Type Interface
-----
10.10.13.1      04:5b:01:01:00:02 03:53:09    Sta  to-ser1
=====
*A:ALU-A#

```

Table 7: Show ARP Table Output Fields

Label	Description
IP Address	The IP address of the ARP entry
MAC Address	The MAC address of the ARP entry
Expiry	The age of the ARP entry
Type	Dyn — the ARP entry is a dynamic ARP entry
	Inv — the ARP entry is an inactive static ARP entry (invalid)
	Oth — the ARP entry is a local or system ARP entry
	Sta — the ARP entry is an active static ARP entry
Interface	The IP interface name associated with the ARP entry
No. of ARP Entries	The number of ARP entries displayed in the list

authentication

Syntax	authentication statistics authentication statistics interface [<i>ip-int-name</i> <i>ip-address</i>] authentication statistics policy <i>name</i>						
Context	show>router>authentication						
Description	This command displays interface or policy authentication statistics.						
Parameters	[<i>ip-int-name</i> <i>ip-address</i>] — specifies an existing interface name or IP address <table><tr><td>Values</td><td><i>ip-int-name</i></td><td>32 chars max</td></tr><tr><td></td><td><i>ip-address</i></td><td>a.b.c.d</td></tr></table> <i>name</i> — specifies an existing policy name	Values	<i>ip-int-name</i>	32 chars max		<i>ip-address</i>	a.b.c.d
Values	<i>ip-int-name</i>	32 chars max					
	<i>ip-address</i>	a.b.c.d					
Output	The following output is an example of the authentication statistics, and Table 8 describes the fields.						

Sample Output

```
*A:ALU-1#show>router>auth# statistics

=====
Authentication Global Statistics
=====
Client Packets Authenticate Fail      : 0
Client Packets Authenticate Ok       : 12
=====
*A:ALU-1#
```

Table 8: Show Authentication Statistics Output Fields

Label	Description
Client Packets Authenticate Fail	The number of packets that failed authentication
Client Packets Authenticate Ok	The number of packets that were authenticated

bfd

Syntax	bfd
Context	show>router
Description	This command enables the context to display bidirectional forwarding detection (BFD) information.

interface

Syntax	interface
Context	show>router>bfd
Description	This command displays BFD interface information.
Output	The following output is an example of BFD interface information, and Table 9 describes the fields.

Sample Output

```
*A:ALU-1# show router bfd interface
=====
BFD Interface
=====
Interface name                Tx Interval    Rx Interval    Multiplier
-----
net10_1_2                     100            100            3
net11_1_2                     100            100            3
net12_1_2                     100            100            3
net13_1_2                     100            100            3
net14_1_2                     100            100            3
net15_1_2                     100            100            3
net16_1_2                     100            100            3
net17_1_2                     100            100            3
net18_1_2                     100            100            3
net19_1_2                     100            100            3
net1_1_2                      100            100            3
net1_2_3                      100            100            3
net20_1_2                     100            100            3
net21_1_2                     100            100            3
net22_1_2                     100            100            3
net23_1_2                     100            100            3
net24_1_2                     100            100            3
net25_1_2                     100            100            3
net2_1_2                      100            100            3
net3_1_2                      100            100            3
net4_1_2                      100            100            3
net5_1_2                      100            100            3
net6_1_2                      100            100            3
net7_1_2                      100            100            3
net8_1_2                      100            100            3
net9_1_2                      100            100            3
-----
No. of BFD Interfaces: 26
```

Table 9: Show BFD Interface Output Fields

Label	Description
TX Interval	Displays the interval, in milliseconds, between the transmitted BFD messages to maintain the session
RX Interval	Displays the expected interval, in milliseconds, between the received BFD messages to maintain the session
Multiplier	Displays the integer used by BFD to declare when the far end is down.

session

Syntax **session** [**src** *ip-address* [**dst** *ip-address* | **detail**]]

Context show>router>bfd

Description This command displays session information.

Parameters *ip-address* — displays the interface information associated with the specified IP address

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

Output The following output is an example of BFD session information, and [Table 10](#) describes the fields.

Sample Output

```
*A:ALU-1# show router bfd session
=====
BFD Session
=====
Interface          State      Tx Intvl  Rx Intvl  Mult
Remote Address     Protocol
-----
net1_1_2           Up (3)     100        100        3
  12.1.2.1         None
net1_2_3           Up (3)     100        100        3
  12.2.3.2         None
  156367          156365
-----
No. of BFD sessions: 2
=====
*A:ALU-1#
```

Table 10: Show BFD Session Output Fields

Label	Description
State	Displays the administrative state for this BFD session
Protocol	Displays the active protocol
Tx Intvl	Displays the interval, in milliseconds, between the transmitted BFD messages to maintain the session
Tx Pkts	Displays the number of transmitted BFD packets
Rx Intvl	Displays the expected interval, in milliseconds, between the received BFD messages to maintain the session
Rx Pkts	Displays the number of received packets
Mult	Displays the integer used by BFD to declare when the neighbor is down

dhcp

Syntax	dhcp
Context	show>router
Description	This command enables the context to display DHCP-related information.

dhcp6

Syntax	dhcp6
Context	show>router
Description	This command enables the context to display DHCPv6-related information.

statistics

Syntax	statistics [interface <i>ip-int-name</i> <i>ip-address</i>]
Context	show>router>dhcp show>router>dhcp6
Description	This command displays statistics for DHCP Relay and DHCPv6 Relay. If no interface name or IP address is specified, then all configured interfaces are displayed.

If an interface name or IP address is specified, then only data regarding the specified interface is displayed.

Parameters *ip-int-name* | *ip-address* — displays statistics for the specified IP interface

Output The following outputs are examples of DHCP statistics information:

- DHCP statistics ([Sample Output](#), [Table 11](#))
- DHCPv6 statistics ([Sample Output](#), [Table 12](#))

Sample Output

```
*A:ALU-1# show router dhcp statistics
=====
DHCP Global Statistics (Router: Base)
=====
Rx Packets                      : 0
Tx Packets                      : 0
Rx Malformed Packets           : 0
Rx Untrusted Packets           : 0
Client Packets Discarded        : 0
Client Packets Relayed          : 0
Server Packets Discarded        : 0
Server Packets Relayed          : 0
=====
*A:ALU-1#
```

Table 11: Show DHCP Statistics Output Fields

Label	Description
DHCP Global Statistics (Router: Base)	
Rx Packets	The number of packets received
Tx Packets	The number of packets transmitted
Rx Malformed Packets	The number of malformed packets received
Rx Untrusted Packets	The number of untrusted packets received
Client Packets Discarded	The number of packets from the DHCP client that were discarded
Client Packets Relayed	The number of packets from the DHCP client that were forwarded

Table 11: Show DHCP Statistics Output Fields (Continued)

Label	Description
Server Packets Discarded	The number of packets from the DHCP server that were discarded
Server Packets Relayed	The number of packets from the DHCP server that were forwarded

Sample Output

```
*A:ALU-1# show router dhcp6 statistics
```

```
=====
DHCP6 statistics (Router: Base)
=====
Msg-type           Rx           Tx           Dropped
-----
1 SOLICIT           0            0            0
2 ADVERTISE          0            0            0
3 REQUEST            0            0            0
4 CONFIRM            0            0            0
5 RENEW              0            0            0
6 REBIND             0            0            0
7 REPLY              0            0            0
8 RELEASE            0            0            0
9 DECLINE            0            0            0
10 RECONFIGURE        0            0            0
11 INFO_REQUEST       0            0            0
12 RELAY_FORW         0            0            0
13 RELAY_REPLY        0            0            0

-----
Dhcp6 Drop Reason Counters :
-----
1 Dhcp6 oper state is not Up on src itf           0
2 Dhcp6 oper state is not Up on dst itf           0
3 Relay Reply Msg on Client Itf                   0
4 Hop Count Limit reached                         0
5 Missing Relay Msg option, or illegal msg type    0
6 Unable to determine destination on client Itf    0
7 Out of Memory                                    0
8 No global Pfx on Client Itf                     0
9 Unable to determine src Ip Addr                  0
10 No route to server                              0
11 Subscr. Mgmt. Update failed                     0
12 Received Relay Forw Message                    0
13 Packet too small to contain valid dhcp6 msg     0
14 Server cannot respond to this message           0
15 No Server Id option in msg from server          0
16 Missing or illegal Client Id option in client msg 0
17 Server Id option in client msg                  0
18 Server DUID in client msg does not match our own 0
19 Client sent message to unicast while not allowed 0
20 Client sent message with illegal src Ip address 0
21 Client message type not supported in pfx delegation 0
```

```

22 Nbr of addrs or pfxs exceeds allowed max (128) in msg          0
23 Unable to resolve client's mac address                        0
24 The Client was assigned an illegal address                   0
25 Illegal msg encoding                                          0
=====
*A:ALU-1#

```

Table 12: Show DHCPv6 Statistics Output Fields

Label	Description
DHCP6 Statistics (Router: Base)	
Msg-type	The number of messages received, transmitted, or dropped by the router for each message type
Dhcp6 Drop Reason Counters	The number of times that a message was dropped for a particular reason

summary

Syntax	summary
Context	show>router>dhcp show>router>dhcp6
Description	This command displays a summary of DHCP and DHCPv6 configuration.
Output	The following outputs are examples of DHCP summary information: <ul style="list-style-type: none"> DHCP summary (Sample Output, Table 13) DHCPv6 summary (Sample Output, Table 14)

Sample Output

```

*A:ALU-48# show router dhcp summary
=====
DHCP Summary (Router: Base)
=====
Interface Name      Arp      Used/      Info      Admin
SapId/Sdp           Populate Provided  Option    State
-----
vprn_interface      No        0/0        Keep      Down
sap:1/5/2           0/0
-----
Interfaces: 1
=====
*A:ALU-48#

```

Table 13: Show DHCP Summary Output Fields

Label	Description
DHCP Summary (Router: Base)	
Interface Name SapID/Sdp	The name of the interface or SAP/SDP identifier
Arp Populate	Specifies whether ARP populate is enabled or disabled
Used/Provided	Used — number of lease-states that are currently in use on the specified interface; that is, the number of clients on the interface that got an IP address by DHCP. This number is always less than or equal to the “Provided” field.
	Provided — lease-populate value configured for the specified interface
Info Option	Keep — the existing information is kept on the packet and the router does not add any additional information
	Replace — on ingress, the existing information-option is replaced with the information-option from the router
	Drop — the packet is dropped and an error is logged
Admin State	The administrative state
Interfaces	The total number of DHCP interfaces

Sample Output

```

*A:ALU-48# show router dhcp6 summary
=====
DHCP6 Summary (Router: Base)
=====
Interface Name      Nbr      Used/Max Relay   Admin  Oper Relay
  SapId            Resol.   Used/Max Server  Admin  Oper Server
-----
iesSap              No        0/0              Down   Down
  sap:1/2/3:801          0/8000          Down   Down
iesintf             No        0/0              Down   Down
  sdp:spoke-5:9999       0/8000          Down   Down
-----
Interfaces: 2
=====
*A:ALU-48#

```

Table 14: Show DHCPv6 Summary Output Fields

Label	Description
DHCP Summary (Router: Base)	
Interface Name SapID	The name of the interface or SAP/SDP identifier
Nbr Resol.	Yes — neighbor resolution (discovery) is enabled
	No — neighbor resolution (discovery) is disabled
Used/Max Relay	Used — number of relay routes currently being used on the interface
	Max Relay — maximum number of relay routes on the interface
Used/Max Server	Used — number of server routes currently being used on the interface
	Max Server — maximum number of server routes currently being used on the interface
Admin	The administrative state
Oper Relay	The operating state of the relay routes
Oper Server	The operating state of the server routes (not applicable in Release 4.0)
Interfaces	The total number of DHCPv6 interfaces

ecmp

Syntax **ecmp**

Context show>router

Description This command displays the ECMP settings for the router.

Output The following output is an example of router ECMP information, and [Table 15](#) describes the fields.

Sample Output

```
*A:ALU-A# show router ecmp
=====
Router ECMP
=====
Instance      Router Name      ECMP      Configured-ECMP-Routes
-----
1             Base             True      8
=====
```


Table 15: Show ECMP Settings Output Fields

Label	Description
Instance	The router instance number
Router Name	The name of the router instance
ECMP	False — ECMP is disabled for the instance
	True — ECMP is enabled for the instance
Configured-ECMP-Routes	The number of ECMP routes configured for path sharing

fib

Syntax **fib** *slot-number* [*family*] [*ip-prefix/prefix-length*] [**longer**] [**secondary**]
fib *slot-number* [*family*] **summary**
fib *slot-number* [**nh-table-usage**]

Context show>router

Description This command displays the active FIB entries for a specific CSM.

Parameters *slot-number* — displays only the routes matching the specified chassis slot number

Values 1

family — displays the router IP interface table

Values **ipv4** — displays only those peers that have the IPv4 family enabled

ipv6 — displays the peers that are IPv6-capable

ip-prefix/prefix-length — displays FIB entries only matching the specified IP prefix and prefix length

Values *ipv4-prefix* a.b.c.d (host bits must be 0)
ipv4-prefix-length 0 to 32

Values *ipv6-prefix* x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D
ipv6-prefix-length 0 to 128

longer — displays FIB entries matching the *ip-prefix/prefix-length* and routes with longer masks

secondary — displays secondary FIB information

summary — displays summary FIB information for the specified slot number

nh-table-usage — displays next-hop table usage

Output The following output is an example of FIB information, and [Table 16](#) describes the fields.

Sample Output

```

*A:ALU-A# show router fib 1 summary

=====
FIB Summary
=====
                                Active
-----
Static                        0
Direct                        0
HOST                          0
BGP                           0
BGP VPN                       0
OSPF                          0
ISIS                          0
RIP                           0
Aggregate                     0
Sub Mgmt                      0
-----
Total                          0
-----
Current Occupancy             0%
Overflow Count                 0
Occupancy Threshold Alerts
    Alert Raised 0 Times;
=====
*A:ALU-A#

```

Table 16: Show FIB Output Fields

Label	Description
Active	The number of active entries in the FIB for each type of route
Total	The total number of active entries in the FIB
Current Occupancy	The percentage of the FIB that is being used; an alert is raised when the percentage exceeds 70% and a clear event is raised when the percentage drops below 65%
Overflow Count	The number of times that the FIB was full
Occupancy Threshold Alerts	The number of times a threshold alert was raised to indicate that more than 70% of the FIB is being used

icmp6

Syntax	icmp6
Context	show>router
Description	This command displays ICMPv6 statistics. ICMPv6 generates error messages to report errors during processing and other diagnostic functions. ICMPv6 packets can be used in the neighbor discovery protocol.
Output	The following output is an example of ICMPv6 information, and Table 17 describes the fields.

Sample Output

```
*A:ALU-A# show router icmp6
=====
Global ICMPv6 Stats
=====
Received

Total                : 0                Errors                : 0
Destination Unreachable : 0                Redirects              : 0
Time Exceeded         : 0                Pkt Too Big           : 0
Echo Request          : 0                Echo Reply             : 0
Router Solicits        : 0                Router Advertisements  : 0
Neighbor Solicits      : 0                Neighbor Advertisements : 0
-----
Sent

Total                : 0                Errors                : 0
Destination Unreachable : 0                Redirects              : 0
Time Exceeded         : 0                Pkt Too Big           : 0
Echo Request          : 0                Echo Reply             : 0
Router Solicits        : 0                Router Advertisements  : 0
Neighbor Solicits      : 0                Neighbor Advertisements : 0
=====
```

Table 17: Show ICMPv6 Output Fields

Label	Description
Total	The total number of all messages received and sent
Destination Unreachable	The number of messages that did not reach the destination
Time Exceeded	The number of messages that exceeded the time threshold
Echo Request	The number of echo requests
Router Solicits	The number of times that the local router was solicited
Neighbor Solicits	The number of times that the neighbor router was solicited

Table 17: Show ICMPv6 Output Fields (Continued)

Label	Description
Errors	The number of error messages
Redirects	The number of packet redirects
Pkt Too Big	The number of packets that exceeded the appropriate size
Echo Reply	The number of echo replies
Router Advertisements	The number of times that the router advertised its location
Neighbor Advertisements	The number of times that the neighbor router advertised its location

interface

Syntax `interface [interface-name]`

Context `show>router>icmp6`

Description This command displays ICMPv6 statistics for all interfaces or for a specified interface.

The following output is an example of ICMPv6 interface information, and [Table 18](#) describes the fields.

Sample Output

```
*A:ALU-A# show router icmp6 interface toSAR_131_121
=====
Interface ICMPv6 Stats
=====
Interface "toSAR_131_121"
-----
Received

Total                : 0                Errors                : 0
Destination Unreachable : 0                Redirects              : 0
Time Exceeded         : 0                Pkt Too Big           : 0
Echo Request          : 0                Echo Reply            : 0
Router Solicits        : 0                Router Advertisements : 0
Neighbor Solicits      : 0                Neighbor Advertisements : 0
-----
Sent

Total                : 0                Errors                : 0
Destination Unreachable : 0                Redirects              : 0
Time Exceeded         : 0                Pkt Too Big           : 0
Echo Request          : 0                Echo Reply            : 0
Router Solicits        : 0                Router Advertisements : 0
```

```
Neighbor Solicits      : 0           Neighbor Advertisements : 0
=====
```

Table 18: Show ICMPv6 Interface Output Fields

Label	Description
Total	The total number of all messages received and sent
Destination Unreachable	The number of messages that did not reach the destination
Time Exceeded	The number of messages that exceeded the time threshold
Echo Request	The number of echo requests
Router Solicits	The number of times that the local router was solicited
Neighbor Solicits	The number of times that the neighbor router was solicited
Errors	The number of error messages
Redirects	The number of packet redirects
Pkt Too Big	The number of packets that exceeded the appropriate size
Echo Reply	The number of echo replies
Router Advertisements	The number of times that the router advertised its location
Neighbor Advertisements	The number of times that the neighbor router advertised its location

interface

Syntax	interface [{ <i>ip-address</i> <i>ip-int-name</i>] [detail] [<i>family</i>] summary exclude-services]
Context	show>router
Description	This command displays the router IP interface table sorted by interface index.
Parameters	<i>ip-address</i> — only displays the interface information associated with the specified IP address
Values	<div> <div><i>ipv4-address</i></div> <div>a.b.c.d (host bits must be 0)</div> </div> <div> <div><i>ipv6-address</i></div> <div> x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D </div> </div>
	<i>ip-int-name</i> — only displays the interface information associated with the specified IP interface

detail — displays detailed IP interface information

summary — displays summary IP interface information for the router

exclude-services — displays IP interface information, excluding IP interfaces configured for customer services. Only core network IP interfaces are displayed.

family — displays the specified router IP interface family

Values **ipv4** — displays only those peers that have the IPv4 family enabled
ipv6 — displays the peers that are IPv6-capable

Output The following outputs are examples of IP interface information:

- standard IP interface information ([Sample Output, Table 19](#))
- detailed IP interface information ([Sample Output, Table 20](#))
- summary IP interface information ([Sample Output, Table 21](#))

Sample Output

```
*A:ALU-1# show router interface
```

```
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm      Opr(v4/v6)  Mode      Port/SapId
IP-Address          PfxState
-----
ip-100.0.0.2        Up        Down/Down   Network  1/1/1
100.10.0.2/10       n/a
system              Up        Down/Down   Network  system
-                   -
to-103              Up        Down/Down   Network  n/a
-                   -
-----
Interfaces : 3
=====
*A:ALU-1#
```

```
*A:ALU-1# show router interface to-103
```

```
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId
IP-Address          PfxState
-----
to-103              Up        Down/Down    Network  n/a
-                   -
-----
```

Table 19: Show Standard IP Interface Output Fields

Label	Description
Interface-Name	The IP interface name
IP-Address	The IP address and subnet mask length of the IP interface n/a — no IP address has been assigned to the IP interface
Adm	Down — the IP interface is administratively disabled
	Up — the IP interface is administratively enabled
Opr (v4/v6)	Down — the IP interface is operationally disabled
	Up — the IP interface is operationally enabled
Mode	Network — the IP interface is a network/core IP interface
Port/SapId	The port or SAP that the interface is bound to

Sample Output

```
*A:ALU-1# show router interface ip-100.0.0.2 detail
```

```
=====
Interface Table (Router: Base)
=====

-----
Interface
-----
If Name       : ip-100.0.0.2
Admin State   : Up
Oper State    : Down
Protocols     : ISIS LDP
IP Addr/mask  : 100.10.0.2/10
Address Type  : Primary
IGP Inhibit   : Disabled
Broadcast Address: Host-ones

-----
Details
-----
If Index      : 3
Last Oper Chg: 04/13/2008 19:35:59
Port Id       : n/a
TOS Marking   : Trusted
Egress Filter : none
SNTP B.Cast   : False
MAC Address   :
IP MTU        : 0
Arp Populate  : Disabled
LdpSyncTimer  : None
Proxy ARP     : Disabled
Rem Proxy ARP : Disabled
Policies      : none

Virt. If Index : 3
Global If Index : 31
If Type        : Network
Ingress Filter : none
QoS Policy     : 1
Arp Timeout    : 14400
ICMP Mask Reply : True
Local Proxy ARP : Disabled
```

```

ICMP Details
Redirects      : Number - 100                      Time (seconds) - 10
Unreachables   : Number - 100                      Time (seconds) - 10
TTL Expired    : Number - 100                      Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr*: Not configured
Peer Pri DNS*: Not configured
Peer Sec DNS*: Not configured
=====
* indicates that the corresponding row element may have been truncated.

*A:ALU-1#

```

Table 20: Show Detailed IP Interface Output Fields

Label	Description
If Name	The IP interface name
Admin State	Down — the IP interface is administratively disabled
	Up — the IP interface is administratively enabled
Oper State	Down — the IP interface is operationally disabled
	Up — the IP interface is operationally enabled
Protocols	The protocol type running on the interface
IP Addr/mask	The IP address and subnet mask length of the IP interface n/a — no IP address has been assigned to the IP interface
Address Type	This is always Primary
If Index	The interface index of the IP router interface
Virt If Index	The virtual interface index of the IP router interface
Last Oper Chg	The last change in operational status
Global If Index	The global interface index of the IP router interface
Port ID	The port identifier
TOS Marking	The TOS byte value in the logged packet
If Type	Network — the IP interface is a network/core IP interface
Egress Filter	Indicates whether egress filters are applied to the port (not applicable in Release 4.0)
Ingress Filter	Indicates whether ingress filters are applied to the port
QoS Policy	The QoS policy ID associated with the IP interface

Table 20: Show Detailed IP Interface Output Fields (Continued)

Label	Description
MAC Address	The MAC address of the IP interface
Arp Timeout	The ARP timeout for the interface, in seconds, which is the time that an ARP entry is maintained in the ARP cache without being refreshed
IP MTU	The IP Maximum Transmission Unit (MTU) for the IP interface
ICMP Mask Reply	False — the IP interface will not reply to a received ICMP mask request
	True — the IP interface will reply to a received ICMP mask request
Arp Populate	Displays if ARP is enabled or disabled
LdpSyncTimer	Specifies the IGP/LDP sync timer value
Redirects	Specifies the maximum number of ICMP redirect messages the IP interface will issue in a given period of time, in seconds Disabled — indicates the IP interface will not generate ICMP redirect messages
Unreachables	Specifies the maximum number of ICMP destination unreachable messages the IP interface will issue in a given period of time, in seconds Disabled — indicates the IP interface will not generate ICMP destination unreachable messages
TTL Expired	Specifies the maximum number (Number) of ICMP TTL expired messages the IP interface will issue in a given period of time, in seconds Disabled — indicates the IP interface will not generate ICMP TTL expired messages

Sample Output

```

*A:ALU-A# show router interface summary
=====
Router Summary (Interfaces)
=====
Instance  Router Name                Interfaces  Admin-Up  Oper-Up
-----
1         Base                        7          7         5
=====
*A:ALU-A#

```

Table 21: Show Summary IP Interfaces Output Fields

Label	Description
Instance	The router instance number
Router Name	The name of the router instance
Interfaces	The number of IP interfaces in the router instance
Admin-Up	The number of administratively enabled IP interfaces in the router instance
Oper-Up	The number of operationally enabled IP interfaces in the router instance

neighbor

Syntax **neighbor** [*ip-int-name* | *ip-address* | **mac** *ieee-mac-address* | **summary**] [**dynamic** | **static** | **managed**]

Context show>router

Description This command displays information about the IPv6 neighbor cache.

Parameters *ip-int-name* — IP interface name

Values 32 characters maximum

ip-address — the address of the IPv6 interface

Values *ipv6-address* x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

ieee-mac-address — the MAC address

Values the 48-bit MAC address in the form *aa:bb:cc:dd:ee:ff* or *aa-bb-cc-dd-ee-ff*, where *aa*, *bb*, *cc*, *dd*, *ee*, and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

summary — displays summary neighbor information

dynamic — displays dynamic IPv6 neighbors

static — displays static IPv6 neighbors

managed — displays managed IPv6 neighbors

Output The following output is an example of IPv6 neighbor information, and [Table 22](#) describes the fields.

Sample Output

```

*A:ALU# show router neighbor
=====
Neighbor Table (Router: Base)
=====
IPv6 Address          State      Interface      Type      RTR
  MAC Address                               Expiry
-----
FE80::203:FAFF:FE78:5C88    STALE      net1_1_2
  00:16:4d:50:17:a3          03h52m08s    Dynamic      Yes
FE80::203:FAFF:FE81:6888    STALE      net1_2_3
  00:03:fa:1a:79:22          03h29m28s    Dynamic      Yes
-----
No. of Neighbor Entries: 2
=====
*A:ALU-A#

```

Table 22: Show IPv6 Neighbor Output Fields

Label	Description
IPv6 Address	The IPv6 address
Interface	The name of the IPv6 interface
MAC Address	The link-layer address
State	The current administrative state
Expiry	The amount of time before the entry expires
Type	The type of IPv6 interface
RTR	Specifies whether the neighbor is a router

route-table

- Syntax** **route-table** [*family*] [*ip-prefix*[/*prefix-length*] [**longer** | **exact**]] | [**protocol** *protocol-name*] | [**summary**]
- Context** show>router
- Description** This command displays the active routes in the routing table.
- If no command line arguments are specified, all routes are displayed, sorted by prefix.
- Parameters** *family* — specifies the type of routing information to be distributed by this peer group
- Values** **ipv4** — displays the routes that have the IPv4 family enabled, excluding IP-VPN routes
- ipv6** — displays the routes that are IPv6-capable, including IPv6 static routes

ip-prefix/prefix-length — displays only those entries matching the specified IP prefix and prefix length

Values	<i>ipv4-prefix</i>	a.b.c.d (host bits must be 0)
	<i>ipv4-prefix-length</i>	0 to 32
Values	<i>ipv6-prefix</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 to FFFF]H
		d: [0 to 255]D
	<i>ipv6-prefix-length</i>	0 to 128

longer — displays routes matching the *ip-prefix/prefix-length* and routes with longer masks

exact — displays the exact route matching the *ip-prefix/prefix-length* masks

protocol-name — displays routes learned from the specified protocol

Values local, static, ospf, isis, aggregate, bgp, bgp-vpn

summary — displays route table summary information

Output The following output is an example of routing table information, and [Table 23](#) describes the fields.

Sample Output

```
*A:ALU# show router route-table
=====
Route Table (Router: Base)
=====
Dest Prefix                                Type    Proto    Age          Pref
  Next Hop[Interface Name]                Metric
-----
10.1.1.1/32                               Local   Local    35d08h00m    0
  system                                   0
-----
No. of Routes: 1
*A:ALU#

*A:ALU-A# show router route-table protocol ospf
=====
Route Table (Router: Base)
=====
Dest Prefix                                Type    Proto    Age          Pref
  Next Hop[Interface Name]                Metric
-----
10.10.0.1/32                               Remote  OSPF     65844        10
  10.10.13.1                               0
-----
*A:ALU-A#
```

Table 23: Show Standard Route Table Output Fields

Label	Description
Dest Prefix	The route destination address and mask
Next Hop	The next hop IP address for the route destination
Type	Local — the route is a local route
	Remote — the route is a remote route
Proto	The protocol through which the route was learned
Age	The route age in seconds for the route
Metric	The route metric value for the route
Pref	The route preference value for the route
No. of Routes	The number of routes displayed in the list

rtr-advertisement

Syntax	rtr-advertisement [interface interface-name] [prefix ipv6-prefix/prefix-length] [conflicts]		
Context	show>router		
Description	This command displays router advertisement information. If no parameters are specified, all routes are displayed, sorted by prefix.		
Parameters	interface-name — the interface name		
	Values	32 characters maximum	
	ipv6-prefix/prefix-length — displays only those routes matching the specified IP prefix and prefix length		
	Values	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
		ipv6-prefix-length	0 to 128
	conflicts — displays router advertisement conflicts		
Output	The following output is an example of router advertisement information, and Table 24 describes the fields.		

Sample Output

```

*A:ALU-A# show router rtr-advertisement
=====
Router Advertisement
-----
Interface: interfaceNetworkNonDefault
-----
Rtr Advertisement Tx : 8                Last Sent           : 00h01m28s
Nbr Solicitation Tx  : 83               Last Sent           : 00h00m17s
Nbr Advertisement Tx : 74               Last Sent           : 00h00m25s
Rtr Advertisement Rx : 8                Rtr Solicitation Rx : 0
Nbr Advertisement Rx : 83               Nbr Solicitation Rx : 74
-----
Max Advert Interval : 601               Min Advert Interval : 201
Managed Config      : TRUE              Other Config         : TRUE
Reachable Time       : 00h00m00s400ms   Router Lifetime      : 00h30m01s
Retransmit Time      : 00h00m00s400ms   Hop Limit            : 63
Link MTU              : 1500
-----
Prefix: 3::/64
Autonomous Flag       : FALSE            On-link flag         : FALSE
Preferred Lifetime    : 07d00h00m       Valid Lifetime       : 30d00h00m
-----
Prefix: 16::/64
Autonomous Flag       : FALSE            On-link flag         : FALSE
Preferred Lifetime    : 49710d06h       Valid Lifetime       : 49710d06h
-----
Advertisement from: FE80::200:FF:FE00:2
Managed Config       : FALSE            Other Config         : FALSE
Reachable Time        : 00h00m00s0ms     Router Lifetime      : 00h30m00s
Retransmit Time       : 00h00m00s0ms     Hop Limit            : 64
Link MTU              : 0
-----
*A:ALU-A#

```

Table 24: Show Router Advertisement Output Fields

Label	Description
Rtr Advertisement Tx/Last Sent	The number of router advertisements sent and the time they were sent
Nbr Solicitation Tx/Last Sent	The number of neighbor solicitation messages sent and the time they were sent
Nbr Advertisement Tx/Last Sent	The number of neighbor advertisements sent and the time they were sent
Rtr Advertisement Rx	The number of router advertisements received
Rtr Solicitation Rx	The number of router solicitation messages received

Table 24: Show Router Advertisement Output Fields (Continued)

Label	Description
Nbr Advertisement Rx	The number of neighbor advertisements received
Nbr Solicitation Rx	The number of neighbor solicitation messages received
Max Advert Interval	The maximum interval between sending router advertisement messages
Min Advert Interval	The minimum interval between sending router advertisement messages
Managed Config	True — DHCPv6 has been configured
	False — DHCPv6 is not available for address configuration
Other Config	True — there are other stateful configurations
	False — there are no other stateful configurations
Reachable Time	The time, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation
Router Lifetime	The router lifetime, in seconds
Retransmit Time	The time, in milliseconds, between retransmitted neighbor solicitation messages
Hop Limit	The current hop limit
Link MTU	The MTU number that the nodes use for sending packets on the link
Autonomous Flag	True — the prefix can be used for stateless address autoconfiguration
	False — the prefix cannot be used for stateless address autoconfiguration
On-link flag	True — the prefix can be used for onlink determination
	False — the prefix cannot be used for onlink determination
Preferred Lifetime	The remaining time, in seconds, that this prefix will continue to be preferred
Valid Lifetime	The length of time, in seconds, that the prefix is valid for the purpose of onlink determination

static-arp

- Syntax** **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]
- Context** show>router
- Description** This command displays the router static ARP table sorted by IP address.
- If no options are present, all ARP entries are displayed.



Note: Multiple MAC addresses can be associated with an interface that is a network port.

- Parameters**
- ip-address* — displays the static ARP entry associated with the specified IP address
 - ip-int-name* — displays the static ARP entry associated with the specified IP interface name
 - ieee-mac-addr* — displays the static ARP entry associated with the specified MAC address

Output The following output is an example of the static ARP table, and [Table 25](#) describes the fields.

Sample Output

```
*A:ALU-A# show router static-arp
=====
ARP Table
=====
IP Address      MAC Address      Expiry      Type Interface
-----
10.200.0.253    00:00:5a:40:00:01 00:00:00    Sta  to-ser1
12.200.1.1      00:00:5a:01:00:33 00:00:00    Inv  to-ser1a
-----
No. of ARP Entries: 1
=====
*A:ALU-A#

*A:ALU-A# show router static-arp 12.200.1.1
=====
ARP Table
=====
IP Address      MAC Address      Expiry      Type Interface
-----
12.200.1.1      00:00:5a:01:00:33 00:00:00    Inv  to-ser1
=====
*A:ALU-A#
```


Table 25: Show Static ARP Table Output Fields

Label	Description
IP Address	The IP address of the static ARP entry
MAC Address	The MAC address of the static ARP entry
Expiry	The age of the ARP entry. Static ARPs always have 00:00:00 for the age.
Type	Inv — the ARP entry is an inactive static ARP entry (invalid)
	Sta — the ARP entry is an active static ARP entry
Interface	The IP interface name associated with the ARP entry
No. of ARP Entries	The number of ARP entries displayed in the list

static-route

Syntax	static-route [<i>family</i>] [<i>ip-prefix/prefix-length</i> preference <i>preference</i> next-hop <i>ip-address</i> tag <i>tag</i>] [detail]		
Context	show>router		
Description	This command displays the static entries in the routing table. If no options are present, all static routes are displayed sorted by prefix.		
Parameters	<i>family</i> — displays the specified router IP interface family		
	Values	ipv4 — displays only those routes that have the IPv4 family enabled	
		ipv6 — displays the routes that are IPv6-capable	
	<i>ip-prefix/prefix-length</i> — displays only those entries matching the specified IP prefix and prefix length		
	Values	<i>ipv4-prefix</i>	a.b.c.d (host bits must be 0)
		<i>ipv4-prefix-length</i>	0 to 32
	Values	<i>ipv6-prefix</i>	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
		<i>ipv6-prefix-length</i>	0 to 128
	<i>preference</i> — only displays static routes with the specified route preference		
	Values	0 to 65535	

ip-address — only displays static routes with the specified next hop IP address

Values *ipv4-address* a.b.c.d (host bits must be 0)

Values *ipv6-address* x:x:x:x:x:x:x:x (eight 16-bit pieces)
 x:x:x:x:x:x:d.d.d.d
 x: [0 to FFFF]H
 d: [0 to 255]D

tag — displays the 32-bit integer tag added to the static route. The tag is used in route policies to control distribution of the route into other protocols.

Values 1 to 4294967295

detail — displays detailed static route information

Output The following output is an example of static route information, and [Table 26](#) describes the fields.

Sample Output

```
*A:ALU-1# show router static-route

=====
Static Route Table (Router: Base)  Family: IPv4
=====
Prefix                               Tag      Met    Pref Type Act
  Next Hop                           Interface
-----
192.168.250.0/24                      1        5     NH   Y
   10.200.10.1                       to-ser1
192.168.252.0/24                      1        5     NH   N
   10.10.0.254                       n/a
192.168.253.0/24                      1        5     NH   N
   to-ser1                           n/a
=====
*A:ALU-A#
```

Table 26: Show Static Route Table Output Fields

Label	Description
Prefix	The static route destination address
Tag	The 32-bit integer tag added to the static route
Met	The route metric value for the static route
Pref	The route preference value for the static route
Type	NH — The route is a static route with a directly connected next hop. The next hop for this type of route is either the next-hop IP address or an egress IP interface name.

Table 26: Show Static Route Table Output Fields (Continued)

Label	Description
Act	N — the static route is inactive; for example, the static route is disabled or the next-hop IP interface is down
	Y — the static route is active
Next Hop	The next hop for the static route destination
No. of Routes	The number of routes displayed in the list

status

Syntax	status
Context	show>router
Description	This command displays the router status.
Output	The following output is an example of router status information, and Table 27 describes the fields.

Sample Output

```
*A:ALU-1# show router status

=====
Router Status (Router: Base)
=====
-----
Admin State      Oper State
-----
Router           Up           Up
OSPFv2-0         Up           Up
ISIS             Up           Up
MPLS             Up           Up
RSVP             Up           Down
LDP              Up           Down
BGP              Up           Up

Max IPv4 Routes  No Limit
Max IPv6 Routes  No Limit
Total IPv4 Routes 5
Total IPv6 Routes 0
ECMP Max Routes  1
Triggered Policies No
=====
*A:ALU-1#
```

Table 27: Show Router Status Output Fields

Label	Description
Router	The administrative and operational states for the router
OSPFv2-0	The administrative and operational states for the OSPF protocol
ISIS	The administrative and operational states for the IS-IS protocol
MPLS	The administrative and operational states for the MPLS protocol
RSVP	The administrative and operational states for the RSVP protocol
LDP	The administrative and operational states for the LDP protocol
BGP	The administrative and operational states for the BGP protocol
Max IPv4 Routes	The maximum number of IPv4 routes configured for the system
Max IPv6 Routes	The maximum number of IPv6 routes configured for the system
Total IPv4 Routes	The number of IPv4 routes in the route table
Total IPv6 Routes	The number of IPv6 routes in the route table
ECMP Max Routes	The number of ECMP routes configured for path sharing
Triggered Policies	No — triggered route policy re-evaluation is disabled
	Yes — triggered route policy re-evaluation is enabled

tunnel-table

Syntax **tunnel-table** [*ip-address[/mask]*] [**protocol** *protocol* | **sdp** *sdp-id*] [**summary**]

Context show>router

Description This command displays tunnel table information.

Note that auto-bind GRE tunnels are not displayed in the **show** command output. GRE tunnels are not the same as SDP tunnels that use the GRE encapsulation type.

Parameters *ip-address/mask* — displays the specified tunnel table's destination IP address and mask

protocol — displays LDP protocol information

sdp-id — displays information about the specified SDP

summary — displays summary tunnel table information

Output The following output is an example of tunnel table information, and [Table 28](#) describes the fields.

Sample Output

```
*A:ALU-1# show router tunnel-table
```

```
=====
Tunnel Table (Router: Base)
=====
Destination      Owner Encap TunnelId Pref    Nexthop    Metric
-----
10.0.0.1/32      sdp   GRE    10     5       10.0.0.1    0
10.0.0.1/32      sdp   GRE    21     5       10.0.0.1    0
10.0.0.1/32      sdp   GRE    31     5       10.0.0.1    0
10.0.0.1/32      sdp   GRE    41     5       10.0.0.1    0
=====
*A:ALU-1#
```

```
*A:ALU-1# show router tunnel-table summary
```

```
=====
Tunnel Table Summary (Router: Base)
=====
                        Active                Available
-----
LDP                     1                  1
SDP                     1                  1
RSVP                    0                  0
=====
*A:ALU-1#
```

Table 28: Show Tunnel Table Output Fields

Label	Description
Destination	The route's destination address and mask
Owner	The tunnel owner
Encap	The tunnel encapsulation type
TunnelID	The tunnel (SDP) identifier
Pref	The route preference for routes learned from the configured peer(s)
Nexthop	The next hop for the route's destination
Metric	The route metric value for the route

Clear Commands

arp

Syntax	arp { all <i>ip-addr</i> interface { <i>ip-int-name</i> <i>ip-addr</i> }}
Context	clear>router
Description	This command clears all or specific ARP entries. The scope of ARP cache entries cleared depends on the command line option(s) specified.
Parameters	all — clears all ARP cache entries <i>ip-addr</i> — clears the ARP cache entry for the specified IP address <i>ip-int-name</i> — clears all ARP cache entries for the IP interface with the specified name interface <i>ip-addr</i> — clears all ARP cache entries for the IP interface with the specified IP address

authentication

Syntax	authentication statistics [interface { <i>ip-int-name</i> <i>ip-address</i> }]
Context	clear>router
Description	This command clears router authentication statistics.
Parameters	<i>ip-int-name</i> — clears the statistics for the specified interface name Values 32 characters maximum <i>ip-address</i> — clears the statistics for the specified IP address Values a.b.c.d

bfd

Syntax	bfd
Context	clear>router
Description	This command enables the context to clear bidirectional forwarding (BFD) sessions and statistics.

session

Syntax	session src-ip <i>ip-address</i> dst-ip <i>ip-address</i> session all
Context	clear>router>bfd
Description	This command clears BFD sessions.
Parameters	src-ip <i>ip-address</i> — specifies the address of the local endpoint of this BFD session dst-ip <i>ip-address</i> — specifies the address of the far-end endpoint of this BFD session all — clears all BFD sessions

statistics

Syntax	statistics src-ip <i>ip-address</i> dst-ip <i>ip-address</i> statistics all
Context	clear>router>bfd
Description	This command clears BFD statistics.
Parameters	src-ip <i>ip-address</i> — specifies the address of the local endpoint of this BFD session dst-ip <i>ip-address</i> — specifies the address of the remote endpoint of this BFD session all — clears statistics for all BFD sessions

dhcp

Syntax	dhcp
Context	clear>router
Description	This command enables the context to clear and reset DHCP entities.

dhcp6

Syntax	dhcp6
Context	clear>router
Description	This command enables the context to clear and reset DHCPv6 entities.

statistics

Syntax	statistics [<i>ip-int-name</i> <i>ip-address</i>]				
Context	clear>router>dhcp clear>router>dhcp6				
Description	This command clears statistics for DHCP and DHCPv6 Relay. If no interface name or IP address is specified, statistics are cleared for all configured interfaces. If an interface name or IP address is specified, statistics are cleared only for that interface.				
Parameters	<i>ip-int-name</i> — 32 characters maximum <i>ip-address</i> — IPv4 or IPv6 address				
Values	<table> <tr> <td><i>ipv4-address</i></td><td>a.b.c.d</td></tr> <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:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D</td></tr> </table>	<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 to FFFF]H d: [0 to 255]D
<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 to FFFF]H d: [0 to 255]D				

icmp6

Syntax	icmp6 all icmp6 global icmp6 interface <i>interface-name</i>
Context	clear>router
Description	This command clears ICMPv6 statistics. If an interface name is specified, statistics are cleared only for that interface.
Parameters	all — all statistics global — global statistics <i>interface-name</i> — 32 characters maximum

interface

Syntax	interface [<i>ip-int-name</i> <i>ip-addr</i>] [icmp]
Context	clear>router
Description	This command clears IP interface statistics.

If no IP interface is specified either by IP interface name or IP address, the command will perform the clear operation on all IP interfaces.

Parameters *ip-int-name* | *ip-addr* — the IP interface name or IP interface address

Default all IP interfaces

icmp — specifies to reset the ICMP statistics for the IP interface(s) used for ICMP rate limiting

neighbor

Syntax **neighbor** [**all** | *ip-address*]
neighbor [**interface** *ip-int-name* | *ip-address*]

Context clear>router

Description This command clears IPv6 neighbor information.

If an IP address or interface name is specified, information is cleared only for that interface.

Parameters **all** — all IPv6 neighbors
ip-address — an IPv6 neighbor address

Values IPv6 address x:x:x:x:x:x:x:x (eight 16-bit pieces)
 x:x:x:x:x:x:d.d.d.d
 x: [0 to FFFF]H
 d: [0 to 255]D

ip-int-name — an IPv6 neighbor interface name, 32 characters maximum

router-advertisement

Syntax **router-advertisement all**
router-advertisement [**interface** *interface-name*]

Context clear>router

Description This command clears router advertisement counters.

If an interface name is specified, counters are cleared only for that interface.

Parameters **all** — all interfaces
interface-name — 32 characters maximum

Debug Commands

destination

Syntax	destination <i>trace-destination</i>
Context	debug>trace
Description	This command specifies the destination of trace messages.
Parameters	<i>trace-destination</i> — the destination to send trace messages to
Values	stdout, console, logger, memory

enable

Syntax	[no] enable
Context	debug>trace
Description	This command enables the trace. The no form of the command disables the trace.

trace-point

Syntax	[no] trace-point [module <i>module-name</i>] [type <i>event-type</i>] [class <i>event-class</i>] [task <i>task-name</i>] [function <i>function-name</i>]
Context	debug>trace
Description	This command adds trace points. The no form of the command removes the trace points.

router

Syntax	router <i>router-instance</i>				
Context	debug				
Description	This command configures debugging for a router instance.				
Parameters	<i>router-instance</i> — the router name or service ID				
Values	<table> <tr> <td><i>router-name</i></td><td>Base, management</td></tr> <tr> <td><i>service-id</i></td><td>1 to 2147483647</td></tr> </table>	<i>router-name</i>	Base, management	<i>service-id</i>	1 to 2147483647
<i>router-name</i>	Base, management				
<i>service-id</i>	1 to 2147483647				
Default	Base				

ip

Syntax	[no] ip
Context	debug>router
Description	This command configures debugging for IP.

arp

Syntax	[no] arp
Context	debug>router>ip
Description	This command enables or disables ARP debugging.

dhcp

Syntax	dhcp [interface <i>ip-int-name</i>]
Context	debug>router>ip
Description	This command enables the context for DHCP debugging.

detail-level

Syntax	detail-level {low medium high} no detail-level
Context	debug>router>ip>dhcp
Description	This command enables debugging for the DHCP tracing detail level. The no form of the command disables debugging.

mode

Syntax	mode {dropped-only ingr-and-dropped egr-ingr-and-dropped} no mode
Context	debug>router>ip>dhcp
Description	This command enables debugging for the DHCP tracing mode. The no form of the command disables debugging.

icmp

Syntax	[no] icmp
Context	debug>router>ip
Description	This command enables or disables ICMP debugging.

icmp6

Syntax	icmp6 [<i>ip-int-name</i>] no icmp6
Context	debug>router>ip
Description	This command enables or disables ICMPv6 debugging. If an interface is specified, debugging only occurs on that interface.
Parameters	<i>ip-int-name</i> — only debugs the specified IP interface Values 32 characters maximum

interface

Syntax	[no] interface [<i>ip-int-name</i> <i>ip-address</i>]		
Context	debug>router>ip		
Description	This command enables or disables debugging for virtual interfaces.		
Parameters	<i>ip-int-name</i> — only debugs the specified IP interface		
	Values	32 characters maximum	
	<i>ip-address</i> — only debugs the specified IPv4 or IPv6 address		
	Values	<i>ipv4-address</i>	a.b.c.d
		<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x.d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

neighbor

Syntax	[no] neighbor
Context	debug>router>ip
Description	This command enables or disables neighbor debugging.

packet

Syntax	packet [<i>ip-int-name</i> <i>ip-address</i>] [headers] [<i>protocol-id</i>] no packet [<i>ip-int-name</i> <i>ip-address</i>]		
Context	debug>router>ip		
Description	This command enables or disables debugging for IP packets.		
Parameters	<i>ip-int-name</i> — only debugs the specified IP interface		
	Values	32 characters maximum	
	<i>ip-address</i> — only debugs the specified IPv4 or IPv6 address		
	Values	<i>ipv4-address</i>	a.b.c.d
		<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x.d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	headers — only debugs the packet header		

protocol-id — specifies the decimal value representing the IP protocol to debug. Common protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form of the command removes the protocol from the criteria.

Values 0 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, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
 * — udp/tcp wildcard

route-table

Syntax **route-table** [*ip-prefix/prefix-length*] [**longer**]
no route-table

Context debug>router>ip

Description This command configures route table debugging.

Parameters *ip-prefix/prefix-length* — the IPv4 or IPv6 prefix

Values	<i>ipv4-prefix</i>	a.b.c.d (host bits must be 0)
	<i>ipv4-prefix-length</i>	0 to 32
Values	<i>ipv6-prefix</i>	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
	<i>ipv6-prefix-length</i>	0 to 128

longer — specifies that the prefix list entry matches any route that matches the specified *ip-prefix* and *prefix-length* values greater than the specified *prefix-length*

Filter Policies

In This Chapter

This chapter provides information about filter policies and management.

Topics in this chapter include:

- [Configuring Filter Policies on page 152](#)
 - [Network and Service Interface-based Filtering on page 153](#)
 - [Filter Policy Entries on page 154](#)
 - [Filter Logs on page 160](#)
- [Configuration Notes on page 161](#)
 - [IP Filters on page 161](#)
 - [IPv6 Filters on page 162](#)
 - [MAC Filters on page 162](#)
 - [Filter Logs on page 163](#)
- [Configuring Filter Policies with CLI on page 165](#)
- [Filter Command Reference on page 185](#)

Configuring Filter Policies

Filter policies (or filters), also referred to as Access Control Lists (ACLs), are sets of rules that can be applied to network interfaces, VLL services (specifically, Ethernet and IP pseudowires), VPLS, VPRN and IES services, and IES in-band management services. Filter policies constrain network or user traffic based on IP or MAC match criteria and determine the action that will be invoked against the subject packet (that is, the default action can be either “drop” or “forward”).

The 7705 SAR supports three types of filter policies: IP filters, MAC filters, and CSM filters.

IP filters are applied to the following entities:

- ingress network interfaces, which affects incoming traffic from the network link
- ingress IES management SAPs, which affects incoming node management traffic
- pseudowire SAPs (Epipes and Ipipes), VPLS SAPs, VPRN SAPs, and IES SAPs, which affects incoming user traffic
- ingress VPLS SDPs (spoke and mesh), which affects incoming traffic from the remote end of the service
- egress VPLS SAPs (Ethernet SAPs only), which affects outgoing user traffic

Ingress filters affect only incoming packets regardless of whether they need to be forwarded to a downstream router or are destined for the 7705 SAR.

IPv6 filters are applied to null or dot1q network interfaces and to IES SAPs.

The 7705 SAR also supports IPv4 and IPv6 CSM filters.

MAC filters are applied to the following entities:

- ingress VPLS SAPs, which affects incoming user traffic
- ingress VPLS SDPs (spoke and mesh), which affects outgoing user traffic

IP and MAC filters scan all traffic and take the appropriate (configured) action against matching packets. Packets that are not filtered by the IP or MAC filters and are destined for the 7705 SAR are then further scanned by the CSM filter, if configured. For information on CSM filters, refer to the 7705 SAR OS System Management Guide, “CSM Filters and CSM Security”.

Configuring an entity with a filter policy is optional. If a network or service interface is not configured with filter policies, all traffic is allowed on the interface. By default, there are no filters associated with interfaces or services. The filters must be explicitly created and associated. When you create a new filter, you must specify a unique filter ID value for each new filter policy as well as each new filter entry and associated actions. The filter entries specify the filter matching criteria. See [Filter Policy Entries](#).

Network and Service Interface-based Filtering

IP and MAC filter policies specify either a forward or a drop action for packets, based on information specified in the match criteria. You can create up to 16 unique IP filter policies per adapter card and up to 96 IP filters per node. Within each filter policy, you can create up to 64 matching entries. The same limits apply to MAC filter policies.

The same IP filter policy can be assigned to any entity (network interfaces, IP pseudowires, Ethernet pseudowires, VPLS services, VPRN services, and IES services), all of which can be configured on the same adapter card. For example, a filter policy defined (*filter-id*) as filter-5 can be assigned to multiple Ipipe SAPs and, simultaneously, to network interfaces on the same adapter card.

A filter policy assigned to an entity on one adapter card can also be assigned to any entity on another adapter card. For example, a filter policy defined as filter-2 can be assigned to an Epipe on an Ethernet Adapter card and to a network interface on another Ethernet Adapter card.

An interface that supports IPv6 can have both IPv4 and IPv6 filters assigned to it; these are counted as two unique filters.

Up to 16 unique IP and 16 unique MAC filter policies are supported per adapter card, and assigning the same filter policy to different entities on a card counts as using one filter policy.

Filter entry matching criteria can be as general or specific as required, but all conditions in the entry must be met in order for the packet to be considered a match and the specified entry action performed. The process stops when the first complete match is found and executes the action defined in the entry, either to drop or forward packets that match the criteria.

Configuration and assignment of IP and MAC filter policies is similar for network interfaces, IES management SAPs, Ethernet and IP pseudowire SAPs, VPLS SAPs, VPRN SAPs, IES SAPs, and VPLS SDPs (spoke and mesh). This guide describes the assignment of filter policies to network interfaces. Refer to the 7705 SAR OS Services Guide, “IP Filters” (under “Ethernet VLL (Epipe) Services” and “IP Interworking VLL (Ipipe) Services”), for information on assigning IP filter policies to SAPs, and to “MAC Filters” (under VPLS Features), for information on assigning MAC filter policies to VPLS SAPs and SDPs.

Filter Policy Entries

A filter policy compares the match criteria specified within a filter entry to packets coming into the system, in the order the entries are numbered in the policy. When a packet matches all the parameters specified in the entry, the system takes the specified action to either drop or forward the packet. If a packet does not match the entry parameters, the packet continues through the filter process and is compared to the next filter entry, and so on.

If the packet does not match any of the entries, the system executes the default action specified in the filter policy, which is to either drop or forward the packet. Each filter policy is assigned a unique filter ID. Each filter policy is defined with:

- scope
- default action (drop or forward)
- description
- at least one filter entry

Each filter entry contains:

- match criteria
- an action

Applying Filter Policies

IPv4 filter policies can be applied at the ingress of network IP interfaces, Ethernet and IP pseudowire SAPs, VPLS SAPs and SDPs (spoke and mesh), VPRN and IES services, and IES in-band management services. IPv6 filter policies can be applied to ingress null or dot1q network interfaces and ingress IES SAPs only. IPv4 filter policies can also be applied at the egress of VPLS SAPs (Ethernet only).

IPv6 filters are supported on null or dot1q network interfaces and on IES SAPs only

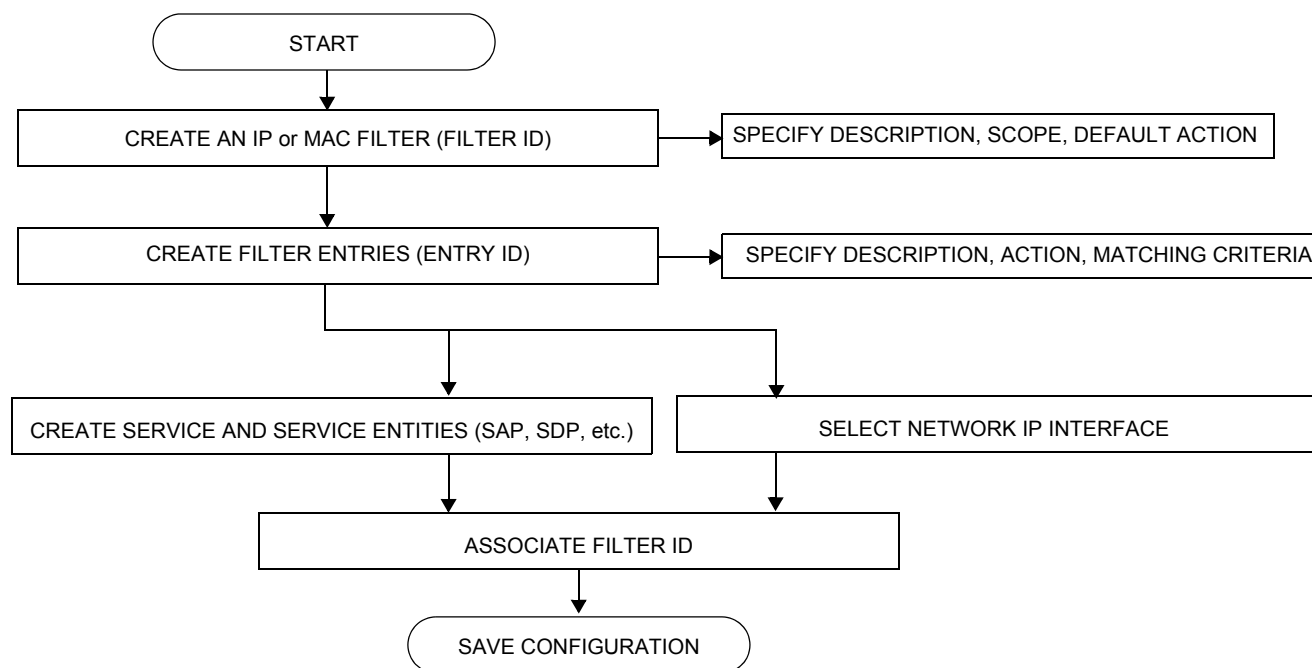
MAC filter policies can be applied at the ingress of VPLS SAPs (Ethernet, and ATM on clear channel OC3 adapter cards) and SDPs (spoke and mesh).



Note: By default, all created filters have a default action of drop (implicit drop). That is, if none of the entries in the filter match the packet, and a default action is not explicitly configured by the user, the packet is dropped.

Figure 3 shows the process to create filter policies and apply them to a network interface.

Figure 3: Creating and Applying Filter Policies



Packet Matching Criteria

Up to 16 IP filter IDs (unique filter policies) can be downloaded per adapter card and up to 96 IP filters per node. The ID can be a value from 1 to 65535. A maximum of 64 filter entries can be defined in each filter policy at the same time. The same limits apply to MAC filters.

All IPv4 filter entries can have as few or as many match parameters specified as required. There are no range-based restrictions on any IPv4 filter entries.

For IPv6 filters, the combined number of fields for all entries in a filter must not exceed 256 bits or 16 fields.

All conditions must be met in order for the packet to be considered a match and the specified action performed. The process stops when the first complete match is found and then executes the action defined in the entry, either to drop or forward packets that match the criteria. If no match is found, the default action is to drop the packet.

IPv4 and IPv6 filter policies compare the match criteria to traffic at a network interface. Matching criteria to drop or forward IP traffic include:

- protocol identifier/next header — For IPv4, a decimal value representing the IP protocol to be used as an IP filter match criterion. Common protocol numbers include ICMP(1), TCP(6), and UDP(17). For IPv6, entering a next header allows the filter to match the first next header following the IPv6 header.
- DSCP name — matching DiffServ Code Point (DSCP) names
- destination IP address and mask — matching destination IP address and mask values (for IPv4) and matching destination IP address and prefix length (for IPv6)
The IPv4 address scheme consists of 32 bits expressed in dotted-decimal notation. The IPv6 address scheme consists of 128 bits expressed in colon-hexadecimal format.
- destination port/range — matching TCP or UDP values
- fragmentation — matching fragmentation state of packets (fragmented or non-fragmented) (not applicable to IPv6)
- ICMP code — matching ICMP code in the ICMP header
- ICMP type — matching ICMP type in the ICMP header
- IP option — matching option or range of options in the IP header (not applicable to IPv6)
- multiple IP options — matching state of multiple option fields in the IP header (true or false) (not applicable to IPv6)
- option present — matching state of the option field in the IP header (present or absent) (not applicable to IPv6)
- source IP address and mask — matching source IP address and mask values (for IPv4) and matching source IP address and prefix length (for IPv6)
The IPv4 address scheme consists of 32 bits expressed in dotted-decimal notation. The IPv6 address scheme consists of 128 bits expressed in colon-hexadecimal format.
- source port/range — matching TCP or UDP port and range values
- TCP ACK — matching state of the ACK bit set in the control bits of the TCP header of an IP packet (set or not set)
- TCP SYN — matching state of the SYN bit set in the control bits of the TCP header of an IP packet (set or not set)



Notes: For IPv6 filters:

- If the source IP address or destination IP address mask is between 1 and 64 (inclusive), 4 out of the 16 available fields are utilized.
- If the source IP address or destination IP address mask is between 65 and 128 (inclusive), 8 out of the 16 available fields are utilized.

MAC filter policies compare the match criteria to traffic at the ingress of a VPLS SAP or SDP (spoke or mesh). Matching criteria to drop or forward MAC traffic include:

- frame type
Entering the frame type allows the filter to match for a specific type of frame format; for example, Ethernet-II will match for only ethernet-II frames.
- source MAC address
Entering the source MAC address allows the filter to search for matching a source MAC address. Enter the source MAC address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 00:dc:98:1d:00:00.
- destination MAC address
Entering the destination MAC address allows the filter to search for matching a destination MAC address. Enter the destination MAC address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 02:dc:98:1d:00:01.
- ethertype
Entering an Ethernet type II Ethertype value to be used as a filter match criterion. The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. The Ethertype accepts decimal, hex, or binary in the range of 1536 to 65535.

Ordering Filter Entries

When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Filter 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.

Packets are compared to entries in a filter policy in ascending entry ID order. To reorder entries in a filter policy, for example, to reposition entry ID 6 as entry ID 2, use the `renum` command (`renum 6 2`).

When a filter policy consists of a single entry, the filter executes actions as follows.

- If a packet matches all the entry criteria, the entry's specified action is performed (drop or forward).
- If a packet does not match all of the entry criteria, the policy's default action is performed (drop or forward).

If a filter policy contains two or more entries, packets are compared in ascending entry ID order (for example, 1, 2, 3 or 10, 20, 30).

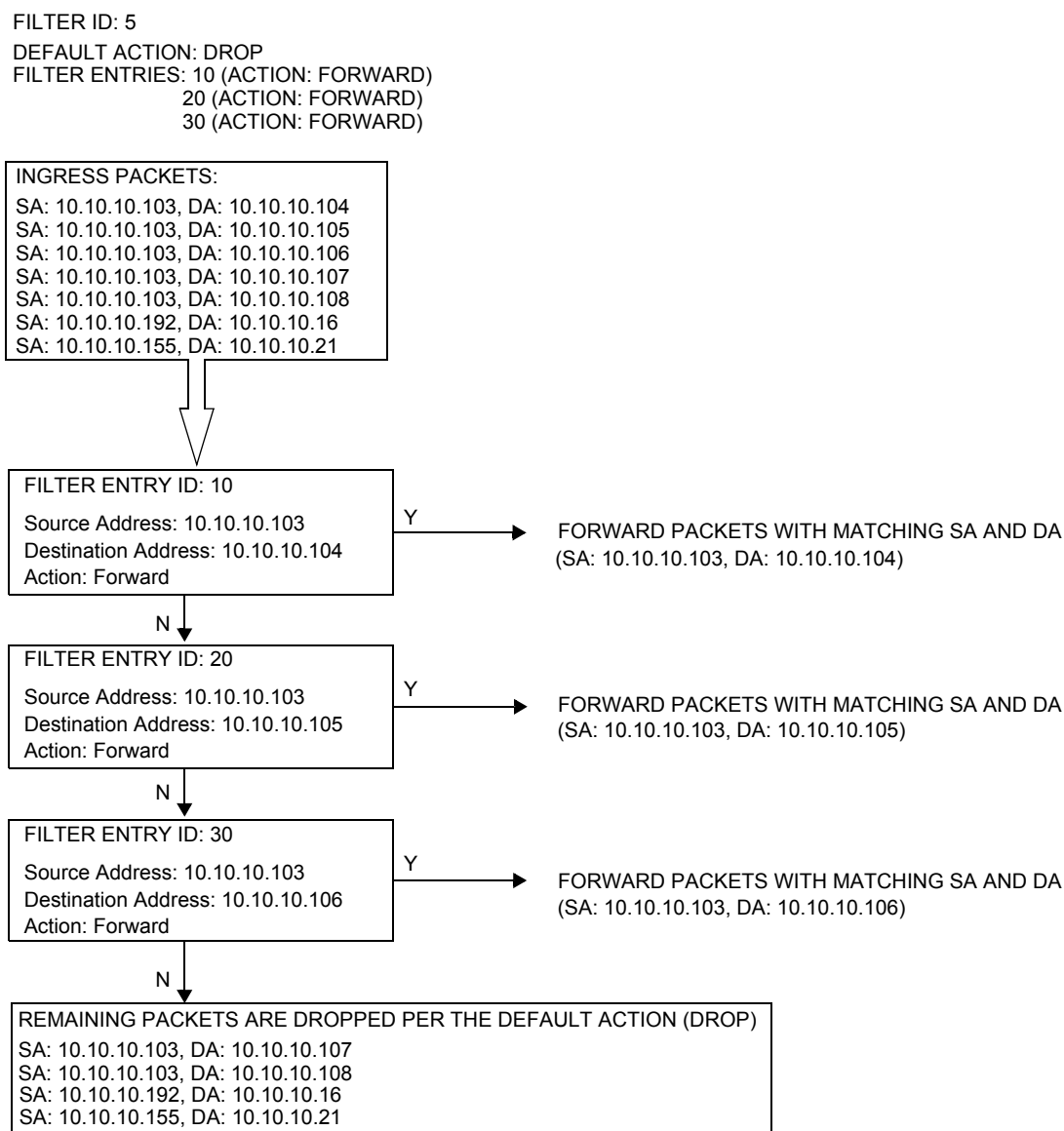
- Packets are compared with the criteria in the first entry ID.
- If a packet matches all the properties defined in the entry, the entry's specified action is executed.
- If a packet does not completely match, the packet continues to the next entry, and then subsequent entries.
- If a packet does not completely match any subsequent entries, the default action is performed (drop or forward).



Note: By default, all created filters have a default action of drop (implicit drop). That is, if none of the entries in the filter match the packet, and a default action is not explicitly configured by the user, the packet is dropped.

Figure 4 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

Figure 4: Filtering Process Example



Filter Logs

Filter entries can be configured to be written to a filter log file. The log file must exist before any entries can be logged. Filter logs can be sent to either memory or to an existing syslog server.

Refer to the 7705 SAR OS System Management Guide, “Syslog”, for information on syslogs.

Configuration Notes

The following information describes the conditions for filter policy implementation.

- Creating a filter policy is optional.
- Using a filter policy is optional.
- A filter policy must be created before it can be applied to a service.
- When a filter policy is configured, it must be defined as having either an *exclusive* scope for one-time use, or a *template* scope meaning that the filter can be applied to multiple interfaces.
- A specific filter must be explicitly associated with a specific interface in order for packets to be matched.
- Each filter policy must consist of at least one filter entry. Each entry represents a collection of filter match criteria. When packets enter an ingress port or SAP or SDP, or exit an egress SAP, the packets are compared to the criteria specified within the entry or entries.
- When you configure a large (complex) filter, it may take a few seconds to load the filter policy configuration.
- The **action** keyword must be entered for the entry to be active. Any filter entry without the **action** keyword will be considered incomplete and will be inactive.

IP Filters

- Define filter entry packet matching criteria — if a filter policy is created with an entry and entry action specified but the packet matching criteria is not defined, then all packets processed through this filter policy entry will pass and take the action specified. There are no default parameters defined for matching criteria.
- Action — an action parameter must be specified for the entry to be active. Any filter entry without an action parameter specified will be considered incomplete and will be inactive.

IPv6 Filters

IPv6 packets with extension headers can be filtered with an IPv6 filter, but are subject to some restrictions:

- if the packet contains the Hop-by-Hop Options header, slow path extraction will occur and the packet will be processed by the CSM's IPv6 filter (if present); therefore, the main (fast path) IPv6 filter will not apply
- if the authentication header is present in the packet and the target fields for the filter are offset by the presence of the authentication header, the filter will not detect the target header fields and no filter action will occur

No alarms, logs, or statistics will be reported in the above cases.

MAC Filters

- If a MAC filter policy is created with an entry and entry action specified but the packet matching criteria is not defined, then all packets processed through this filter policy entry will pass and take the action specified. There are no default parameters defined for matching criteria.
- MAC filters cannot be applied to network interfaces, routable VPRN or IES services.
- Some of the MAC match criteria fields are exclusive to each other, based on the type of Ethernet frame. Use [Table 29](#) to determine the exclusivity of fields.

Table 29: MAC Match Criteria Exclusivity Rules

Frame Format	EtherType
Ethernet – II	Yes
802.3	No
802.3 – snap	No

Filter Logs

- Summarization logging is the collection and summarization of log messages for one specific log ID within a period of time.
- The filter log can be applied to IP filters, MAC filters, service filters, or CPM filters.
- For VPLS scenarios, both Layer 2 and Layer 3 are applicable.
 - Layer 2: source MAC or optionally destination MAC
 - Layer 3: source IPv6 or optionally destination IPv6 for Layer 3 filters
- The summarization interval is 100 s.
- Upon activation of a fixed summarization interval, a mini-table with source/destination address and count is created for each filter type (IP, MAC, or CPM).
- Every received log packet is examined for the source or destination address.
- If the log packet (source/destination address) matches a source/destination address entry in the mini-table (a packet received previously), the summary counter of the matching address is incremented.

Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to [Standards and Protocol Support](#).

Configuring Filter Policies with CLI

This section provides information to configure and manage filter policies using the command line interface.

Topics in this section include:

- [Basic Configuration on page 166](#)
- [Common Configuration Tasks on page 167](#)
 - [Creating an IPv4 or IPv6 Filter Policy on page 167](#)
 - [Creating a MAC Filter Policy on page 172](#)
 - [Configuring Filter Log Policies on page 175](#)
 - [Applying IP and MAC Filter Policies on page 175](#)
 - [Applying Filter Policies to Network Interfaces on page 177](#)
- [Filter Management Tasks on page 178](#)
 - [Renumbering Filter Policy Entries on page 178](#)
 - [Modifying an IP Filter Policy on page 180](#)
 - [Modifying a MAC Filter Policy on page 181](#)
 - [Removing and Deleting a Filter Policy on page 182](#)
 - [Deleting a Filter on page 183](#)

Basic Configuration

The most basic IPv4, IPv6, and MAC filter policy must have the following:

- a filter ID
 - template scope, either *exclusive* or *template*
 - default action (drop or forward)
 - at least one filter entry
 - specified action, either drop or forward
 - specified matching criteria
-

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed for IP filter configuration and provides the CLI commands.

- [Creating an IPv4 or IPv6 Filter Policy](#)
- [Creating a MAC Filter Policy](#)
- [Configuring Filter Log Policies](#)
- [Applying IP and MAC Filter Policies](#)
- [Applying Filter Policies to Network Interfaces](#)

Creating an IPv4 or IPv6 Filter Policy

Configuring and applying filter policies is optional. Each filter policy must have the following:

- the filter type specified (IP)
- a filter policy ID
- a default action (drop or forward)
- template scope specified, either *exclusive* or *template*
- at least one filter entry with matching criteria specified

IP Filter Policy

Use the following CLI syntax to create an IPv4 or IPv6 filter policy template:

CLI Syntax: `config>filter# ip-filter filter-id [create]
description description-string
scope {exclusive|template}
default-action drop`

Example: `config>filter# ip-filter 12 create
config>filter# description "IP-filter"
config>filter$ scope template`

CLI Syntax: `config>filter# ipv6-filter ipv6-filter-id [create]
description description-string
scope {exclusive|template}
default-action drop`

Example: `config>filter# ipv6-filter 10 create`

```
config>filter# description "IPv6-filter"  
config>filter$ scope template
```

The following example displays a template filter policy configuration.

```
A:ALU-7>config>filter# info  
-----  
...  
    ip-filter 12 create  
        description "IP-filter"  
        scope template  
    exit  
...  
-----  
A:ALU-7>config>filter#
```

Use the following CLI syntax to create an exclusive IPv4 or IPv6 filter policy:

CLI Syntax: `config>filter# ip-filter filter-id
description description-string
scope {exclusive|template}
default-action drop`

Example: `config>filter# ip-filter 11 create
config>filter# description "filter-main"
config>filter# scope exclusive`

CLI Syntax: `config>filter# ipv6-filter ipv6-filter-id
description description-string
scope {exclusive|template}
default-action drop`

Example: `config>filter# ipv6-filter 9 create
config>filter# description "ipv6-filter-main"
config>filter# scope exclusive`

The following example displays an exclusive filter policy configuration.

```
A:ALU-7>config>filter# info  
-----  
...  
    ip-filter 11 create  
        description "filter-main"  
        scope exclusive  
    exit  
...  
-----  
A:ALU-7>config>filter#
```


IP Filter Entry

Within a filter policy, configure filter entries that contain criteria against which ingress, egress, and network traffic is matched. The action specified in the entry determine how the packets are handled, either dropped or forwarded.

- Enter a filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria.

Use the following CLI syntax to create an IP filter entry:

CLI Syntax: `config>filter# ip-filter filter-id [create]
entry entry-id
description description-string`

Example: `config>filter# ip-filter 11
config>filter>ip-filter# entry 10 create
config>filter>ip-filter>entry$ description "no-91"
config>filter>ip-filter>entry# exit`

CLI Syntax: `config>filter# ipv6-filter ipv6-filter-id [create]
entry entry-id
description description-string`

Example: `config>filter# ipv6-filter 9
config>filter>ipv6-filter# entry 10 create
config>filter>ipv6-filter>entry$ description "no-91"
config>filter>ipv6-filter>entry# exit`

The following example displays an IP filter entry configuration.

```
A:ALU-7>config>filter>ip-filter# info
-----
description "filter-main"
scope exclusive
entry 10 create
description "no-91"
match
exit
-----
A:ALU-7>config>filter>ip-filter#
```

IP Filter Entry Matching Criteria

Use the following CLI syntax to configure IPv4 filter matching criteria:

CLI Syntax:

```
config>filter>ip-filter>entry#
match
    dscp dscp-name
    dst-ip {ip-address/mask|ip-address netmask}
    dst-port {{lt|gt|eq} dst-port-number} | {range start
        end}
    fragment {true|false}
    icmp-code icmp-code
    icmp-type icmp-type
    ip-option ip-option-value [ip-option-mask]
    multiple-option {true|false}
    option-present {true|false}
    src-ip {ip-address/mask|ip-address netmask}
    src-port {{lt|gt|eq} src-port-number} | {range start
        end}
    tcp-ack {true|false}
    tcp-syn {true|false}
```

Example:

```
config>filter>ip-filter>entry# match
config>filter>ip-filter>entry>match# src-ip
10.10.10.10/32
config>filter>ip-filter>entry>match# dst-ip
10.10.10.91/24
config>filter>ip-filter>entry>match# exit
```

The following example displays a matching configuration.

```
A:ALU-7>config>filter>ip-filter# info
-----
description "filter-main"
scope exclusive
entry 10 create
    description "no-91"
    match
        dst-ip 10.10.10.91/24
        src-ip 10.10.10.10/32
    exit
    action forward
exit
-----
A:ALU-7>config>filter>ip-filter#
```

Use the following CLI syntax to configure IPv6 filter matching criteria:

CLI Syntax:

```
config>filter>ipv6-filter>entry#
match
    dscp dscp-name
    dst-ip {ip-address/prefix-length}
    dst-port {{lt|gt|eq} dst-port-number} | {range start
        end}
    icmp-code icmp-code
    icmp-type icmp-type
    src-ip {ip-address/prefix-length}
    src-port {{lt|gt|eq} src-port-number} | {range start
        end}
    tcp-ack {true|false}
    tcp-syn {true|false}
```

Example:

```
config>filter>ipv6-filter>entry# match
config>filter>ipv6-filter>entry>match# src-ip
11::12/128
config>filter>ipv6-filter>entry>match# dst-ip
13::14/128
config>filter>ipv6-filter>entry>match# exit
```

The following example displays a matching configuration.

```
A:ALU-7>config>filter>ipv6-filter# info
-----
description "ipv6-filter-main"
scope exclusive
entry 10 create
    description "no-91"
    match
        dst-ip 13::14/128
        src-ip 11::12/128
    exit
    action forward exit
-----
A:ALU-7>config>filter>ipv6-filter#
```

Creating a MAC Filter Policy

Configuring and applying filter policies is optional. Each filter policy must have the following:

- The filter type specified (MAC).
- A filter policy ID.
- A default action, either drop or forward.
- Filter policy scope, either exclusive or template.
- At least one filter entry.
- Matching criteria specified.

MAC Filter Policy

Use the following CLI syntax to configure a MAC filter with exclusive scope:

CLI Syntax: `configure>filter>mac-filter filter-id [create]`
`configure>filter>mac-filter# description description-string`
`configure>filter>mac-filter# scope {exclusive | template}`

Example: `configure>filter>mac-filter 90 create`
`configure>filter>mac-filter# description filter-west`
`configure>filter>mac-filter# scope exclusive`

The following example displays an exclusive scope configuration.

```
A:ALU-7>config>filter# info
-----
...
    mac-filter 90 create
        description "filter-west"
        scope exclusive
    exit
-----
A:ALU-7>config>filter#
```

MAC Filter Entry

Within a filter policy, configure filter entries which contain criteria against which ingress, egress, or network traffic is matched. The action specified in the entry determine how the packets are handled, either dropped or forwarded.

- Enter a filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria.

Use the following CLI syntax to configure a MAC filter entry:

CLI Syntax:

```
configure>filter>mac-filter filter-id
configure>filter>mac-filter# entry entry-id [create]
configure>filter>mac-filter>entry# description
description-string
configure>filter>mac-filter>entry# exit
```

Example:

```
configure>filter>mac-filter 90
configure>filter>mac-filter# entry 1 create
configure>filter>mac-filter>entry# description "allow-104"
configure>filter>mac-filter>entry# exit
```

The following example displays a MAC filter entry configuration.

```
A:sim1>config>filter# info
-----
      mac-filter 90 create
        entry 1 create
          description "allow-104"
          match
          exit
          action drop
        exit
      exit
-----
A:sim1>config>filter#
```

MAC Entry Matching Criteria

Use the following CLI syntax to configure a MAC filter entry with matching criteria:

CLI Syntax:

```
configure>filter>mac-filter filter-id
configure>filter>mac-filter# entry entry-id
configure>filter>mac-filter>entry# match [frame-type
{802dot3|802dot2-llc|802dot2-snap|ethernet_II}]
configure>filter>mac-filter>entry>match# src-mac ieee-
address
configure>filter>mac-filter>entry>match# dst-mac ieee-
address
configure>filter>mac-filter>entry>match# etype
0x0600..0xffff
```

Example:

```
configure>filter>mac-filter 90
configure>filter>mac-filter# entry 1
configure>filter>mac-filter>entry# match frame-type
802dot3
configure>filter>mac-filter>entry>match# src-mac
00:dc:98:1d:00:00
configure>filter>mac-filter>entry>match# dst-mac
02:dc:98:1d:00:01
configure>filter>mac-filter>entry>match# etype 0x8100
```

The following example displays a filter matching configuration.

```
A:ALU-7>config>filter# info
-----
description "filter-west"
scope exclusive
entry 1 create
description "allow-104"
match
src-mac 00:dc:98:1d:00:00 ff:ff:ff:ff:ff:ff
dst-mac 02:dc:98:1d:00:01 ff:ff:ff:ff:ff:ff
etype 0x8100
exit
action drop
exit
-----
A:ALU-7>config>filter#
```

Configuring Filter Log Policies

Use the following CLI syntax to configure filter log policy:

CLI Syntax:

```
config>filter# log log-id
        description description-string
        destination memory num-entries
        destination syslog syslog-id
        summary
            no shutdown
            summary-crit dst-addr
            summary-crit src-addr
        wrap-around
```

The following example displays a filter log configuration.

```
A:ALU-48>config>filter>log# info detail
-----
        description "Test filter log."
        destination memory 1000
        wrap-around
        no shutdown
-----
A:ALU-48>config>filter>log#
```

Applying IP and MAC Filter Policies

Filter policies must be created before they can be applied to a service. Create filter policies from the **configure>filter** context.

Use the following CLI syntax to configure an IP and a MAC filter policy for a VPLS service:

CLI Syntax:

```
config>service# vpls service-id
        sap sap-id
            egress
                filter ip ip-filter-id
            ingress
                filter ip ip-filter-id
                filter mac mac-filter-id
        mesh-sdp sdp-id:vc-id [vc-type {ether | vlan}]
            ingress
                filter ip ip-filter-id
                filter mac mac-filter-id
        spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}]
            ingress
                filter ip ip-filter-id
                filter mac mac-filter-id
```

Example:

```
config>service# vpls 5000
config>service>vpls# sap 1/5/5
config>service>vpls>sap# egress filter mac 92
config>service>vpls>sap# ingress filter ip 10
config>service>vpls>sap# exit
config>service>vpls# mesh-sdp 15:5000
config>service>vpls>mesh-sdp# ingress filter mac 93
config>service>vpls>mesh-sdp# exit
config>service>vpls# spoke-sdp 15:5001
config>service>vpls>spoke-sdp# ingress filter mac 94
config>service>vpls>spoke-sdp# exit
```

The following example displays an IP and MAC filter assignment for a VPLS service configuration:

```
A:ALU-48>config>service>vpls# info
-----
...
    sap 1/5/5 create
        ingress
            filter ip 10
        exit
        egress
            filter mac 92
        exit
    exit
    mesh-sdp 15:5000 create
        ingress
            filter mac 93
        exit
    exit
    spoke-sdp 15:5001 create
        ingress
            filter mac 94
        exit
    exit
    no shutdown
...
-----
A:ALU-48>config>service>vpls#
```


Applying Filter Policies to Network Interfaces

IP filter policies can be applied to ingress network IP interfaces.

Filter policies must be created before they can be applied to a service. Create filter policies from the **configure>filter** context.

Apply a Filter Policy to an Interface

CLI Syntax: `config>router# interface ip-int-name
ingress
filter ip ip-filter-id`

CLI Syntax: `config>router# interface ip-int-name
ingress
filter ipv6 ipv6-filter-id`

Example: `config>router# interface to-104
config>router>if# ingress
config>router>if>ingress# filter ip 10
config>router>if# exit`

```
A:ALU-48>config>router# info
#-----
# IP Configuration
#-----
...
    interface "to-104"
      address 10.0.0.10/32
      port 1/1/1
      ingress
        filter ip 10
      exit
    exit
...
#-----
A:ALU-48>config>router#
```

Filter Management Tasks

This section discusses the following filter policy management tasks:

- [Renumbering Filter Policy Entries](#)
- [Modifying an IP Filter Policy](#)
- [Modifying a MAC Filter Policy](#)
- [Removing and Deleting a Filter Policy](#)
- [Deleting a Filter](#)

Renumbering Filter Policy Entries

The 7705 SAR OS exits the matching process when the first match is found and then executes the actions in accordance with the specified action. Because the ordering of entries is important, the numbering sequence can be rearranged. Entries should be numbered from the most explicit to the least explicit.

Use the following CLI syntax to resequence existing IP and MAC filter entries:

CLI Syntax: `config>filter
ip-filter filter-id
renum old-entry-id new-entry-id`

Example: `config>filter>ip-filter# renum 10 15
config>filter>ip-filter# renum 30 40
config>filter>ip-filter# renum 40 1`

CLI Syntax: `config>filter
ipv6-filter ipv6-filter-id
renum old-entry-id new-entry-id`

Example: `config>filter>ipv6-filter# renum 10 15
config>filter>ipv6-filter# renum 30 40
config>filter>ipv6-filter# renum 40 1`

CLI Syntax: `config>filter
mac-filter filter-id
renum old-entry-id new-entry-id`

Example: `config>filter>mac-filter# renum 10 15
config>filter>mac-filter# renum 30 40
config>filter>mac-filter# renum 40 1`

The following output displays the original filter entry order on the left side and the reordered filter entries on the right side:

```
A:ALU-7>config>filter# info
-----
...
    ip-filter 11 create
        description "filter-main"
        scope exclusive
        entry 10 create
            description "no-91"
            match
                dst-ip 10.10.10.91/24
                src-ip 10.10.10.10/32
            exit
            action forward
        exit
    entry 30 create
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.0.100/24
        exit
        action drop
    exit
    entry 35 create
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.0.200/24
        exit
        action forward
    exit
    entry 40 create
        match
            dst-ip 10.10.10.0/29
            src-ip 10.10.10.106/24
        exit
        action drop
    exit
exit
...
-----
A:ALU-7>config>filter#
```

```
A:ALU-7>config>filter# info
-----
...
    ip-filter 11 create
        description "filter-main"
        scope exclusive
        entry 1 create
            match
                dst-ip 10.10.10.0/29
                src-ip 10.10.10.106/24
            exit
            action drop
        exit
    entry 15 create
        description "no-91"
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.0.10/32
        exit
        action forward
    exit
    entry 35 create
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.10.200/24
        exit
        action forward
    exit
    entry 40 create
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.0.100/24
        exit
        action drop
    exit
exit
...
-----
A:ALU-7>config>filter#
```

Modifying an IP Filter Policy

To access a specific IPv4 or IPv6 filter, you must specify the filter ID. Use the `no` form of the command to remove the command parameters or return the parameter to the default setting.

Example:

```
config>filter>ip-filter# description "New IP filter info"
config>filter>ip-filter# entry 2 create
config>filter>ip-filter>entry# description "new entry"
config>filter>ip-filter>entry# action drop
config>filter>ip-filter>entry# match dst-ip
10.10.10.104/32
config>filter>ip-filter>entry# exit
config>filter>ip-filter#
```

Example:

```
config>filter>ipv6-filter# description "IPv6 filter info"
config>filter>ipv6-filter# entry 3 create
config>filter>ipv6-filter>entry# description "new entry"
config>filter>ipv6-filter>entry# action drop
config>filter>ipv6-filter>entry# match dst-ip
10::12/128
config>filter>ipv6-filter>entry# exit
config>filter>ipv6-filter#
```

The following output displays a modified IP filter output.

```
A:ALU-7>config>filter# info
-----
..
ip-filter 11 create
description "New IP filter info"
scope exclusive
entry 1 create
match
dst-ip 10.10.10.0/29
src-ip 10.10.10.106/24
exit
action drop
exit
entry 2 create
description "new entry"
match
dst-ip 10.10.10.104/32
exit
action drop
exit
entry 15 create
description "no-91"
match
dst-ip 10.10.10.91/24
src-ip 10.10.10.10/32
exit
action forward
```

```

        exit
    entry 35 create
        match
            dst-ip 10.10.10.91/24
            src-ip 10.10.0.200/24
        exit
        action forward
    exit
exit
..
-----
A:ALU-7>config>filter#

```

Modifying a MAC Filter Policy

To access a specific MAC filter, you must specify the filter ID. Use the **no** form of the command to remove the command parameters or return the parameter to the default setting.

Example:

```

config>filter# mac-filter 90 create
config>filter>mac-filter# description "New mac filter"
config>filter>mac-filter# entry 1 create
config>filter>mac-filter>entry# description "New mac
entry"
config>filter>mac-filter>entry# action forward
config>filter>mac-filter>entry# exit

```

The following output displays the modified MAC filter output:

```

A:ALU-7>config>filter# info
-----
...
    mac-filter 90 create
        description "New mac filter"
        scope exclusive
        entry 1 create
            description "New mac entry"
            match
                src-mac 00:dc:98:1d:00:00
                dst-mac 02:dc:98:1d:00:01
            exit
            action forward
        exit
    exit
...
-----
A:ALU-7>config>filter#

```

Removing and Deleting a Filter Policy

Before you can delete a filter, you must remove the filter association from the applied ingress and egress SAPs, ingress SDPs, and ingress network interfaces.

You can remove a filter policy and then delete it from the following entities:

- [Removing a Filter from an Ingress SAP or Ingress VPLS SDP](#)
- [Removing a Filter from an Egress Ethernet VPLS SAP](#)
- [Removing a Filter from a Network Interface](#)

Removing a Filter from an Ingress SAP or Ingress VPLS SDP

To remove an IP or MAC filter from an ingress SAP or ingress VPLS SDP (spoke or mesh), enter the following CLI commands:

CLI Syntax:

```
config>service# vpls service-id
    sap port-id
    ingress
        no filter [ip ip-filter-id | mac mac-filter-id]
    spoke-sdp sdp-id:vc-id
    ingress
        no filter [ip ip-filter-id | mac mac-filter-id]
    mesh-sdp sdp-id:vc-id
    ingress
        no filter [ip ip-filter-id | mac mac-filter-id]
```

Example:

```
config>service# vpls 5000
config>service>vpls# sap 1/1/2
config>service>vpls>sap# ingress
config>service>vpls>sap>ingress# no filter ip 232
config>service>vpls>sap>ingress# exit
config>service>vpls>sap# exit
config>service>vpls>spoke-sdp 15:5001
config>service>vpls>spoke-sdp# ingress
config>service>vpls>spoke-sdp>ingress# no filter mac 55
config>service>vpls>spoke-sdp>ingress# exit
config>service>vpls>spoke-sdp# exit
config>service>vpls>mesh-sdp 15:5000
config>service>vpls>mesh-sdp# ingress
config>service>vpls>mesh-sdp>ingress# no filter mac 54
```

Removing a Filter from an Egress Ethernet VPLS SAP

To remove an IP filter from an egress Ethernet VPLS SAP, enter the following CLI commands:

CLI Syntax: `config>service# vpls service-id
sap port-id
egress
no filter ip ip-filter-id`

Example: `config>service# vpls 5000
config>service>vpls# sap 1/1/2
config>service>vpls>sap# egress
config>service>vpls>sap>egress# no filter ip 232`

Removing a Filter from a Network Interface

To delete an IPv4 or IPv6 filter from a network interface, enter the following CLI commands:

CLI Syntax: `config>router# interface ip-int-name
ingress
no filter [ip ip-filter-id | ipv6 ipv6-filter-id]`

Example: `config>router# interface b11
config>router>if# ingress
config>filter>if>ingress# no filter ip 2
config>filter>if>ingress# exit`

Deleting a Filter

After you have removed the filter from all the network interfaces, SAPs, and SDPs (spoke and mesh) where it was applied, use the following CLI syntax to delete the filter:

CLI Syntax: `config>filter# no ip-filter filter-id`

CLI Syntax: `config>filter# no ipv6-filter ipv6-filter-id`

CLI Syntax: `config>filter# no mac-filter filter-id`

Example: `config>filter# no ip-filter 2
config>filter# no mac-filter 55`

Filter Command Reference

Command Hierarchies

- [Configuration Commands](#)
 - [IP Filter Log Configuration Commands](#)
 - [IP Filter Policy Configuration Commands](#)
 - [IPv6 Filter Policy Configuration Commands](#)
 - [MAC Filter Policy Commands](#)
- [Show Commands](#)
- [Clear Commands](#)
- [Monitor Commands](#)

Configuration Commands

IP Filter Log Configuration Commands

```

config
  — filter
    — log log-id [create]
    — no log log-id
      — description description-string
      — no description
      — destination memory num-entries
      — destination syslog syslog-id
      — no destination
      — [no] shutdown
      — summary
        — [no] shutdown
        — summary-crit dst-addr
        — summary-crit src-addr
        — no summary-crit
      — [no] wrap-around

```

IP Filter Policy Configuration Commands

```

config
  — filter
    — ip-filter filter-id [create]
    — no ip-filter filter-id
      — default-action {drop | forward}
      — description description-string
      — no description
      — entry entry-id [create]
      — no entry entry-id
        — action {drop | forward}
        — no action
        — description description-string
        — no description
        — log log-id
        — no log
        — match [protocol protocol-id]
        — no match
          — dscp dscp-name
          — no dscp
          — dst-ip {ip-address/mask | ip-address netmask}
          — no dst-ip
          — dst-port {lt | gt | eq} dst-port-number
          — dst-port range start end
          — no dst-port
          — fragment {true | false}
          — no fragment
          — icmp-code icmp-code
          — no icmp-code

```

```

— icmp-type icmp-type
— no icmp-type
— ip-option ip-option-value [ip-option-mask]
— no ip-option
— multiple-option {true | false}
— no multiple-option
— option-present {true | false}
— no option-present
— src-ip {ip-address/mask | ip-address netmask}
— no src-ip
— src-port {lt | gt | eq} src-port-number
— src-port range start end
— no src-port
— tcp-ack {true | false}
— no tcp-ack
— tcp-syn {true | false}
— no tcp-syn
— renum old-entry-id new-entry-id
— scope {exclusive | template}
— no scope

```

IPv6 Filter Policy Configuration Commands

```

config
— filter
— ipv6-filter ipv6-filter-id [create]
— no ipv6-filter ipv6-filter-id
— default-action {drop | forward}
— description description-string
— no description
— entry entry-id [create]
— no entry entry-id
— action {drop | forward}
— no action
— description description-string
— no description
— log log-id
— no log
— match [next-header next-header]
— no match
— dscp dscp-name
— no dscp
— dst-ip ipv6-address/prefix-length
— no dst-ip
— dst-port {lt | gt | eq} dst-port-number
— dst-port range start end
— no dst-port
— icmp-code icmp-code
— no icmp-code
— icmp-type icmp-type
— no icmp-type
— src-ip ipv6-address/prefix-length

```

- **no src-ip**
- **src-port** {lt | gt | eq} *src-port-number*
- **src-port range** *start end*
- **no src-port**
- **tcp-ack** {true | false}
- **no tcp-ack**
- **tcp-syn** {true | false}
- **no tcp-syn**
- **renum** *old-entry-id new-entry-id*
- **scope** {exclusive | template}
- **no scope**

MAC Filter Policy Commands

```

config
  — filter
    — mac-filter filter-id [create]
    — no mac-filter filter-id
      — default-action {drop | forward}
      — description description-string
      — no description
      — entry entry-id [create]
      — no entry entry-id
        — action {drop | forward}
        — no action
        — description description-string
        — no description
        — log log-id
        — no log
        — match frame-type {802dot3 | 802dot2-llc | 802dot2-snap | ethernet_II}
        — no match
          — — dst-mac ieee-address
          — — no dst-mac
          — — etype 0x0600..0xffff
          — — no etype
          — — src-mac ieee-address
          — — no src-mac
      — renum old-entry-id new-entry-id
      — scope {exclusive | template}
      — no scope

```

Show Commands

```
show
  — filter
    — ip [ip-filter-id | ipv6-filter-id] [entry entry-id] [association | counters]
    — log [bindings]
    — log log-id [match string]
    — mac {mac-filter-id} [entry entry-id] [association | counters]
```

Clear Commands

```
clear
  — filter
    — ip ip-filter-id [entry entry-id] [ingress | egress]
    — ipv6 ipv6-filter-id [entry entry-id] [ingress | egress]
    — log log-id
    — mac mac-filter-id [entry entry-id] [ingress | egress]
```

Monitor Commands

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

Command Descriptions

- [Configuration Commands on page 191](#)
- [Show Commands on page 216](#)
- [Clear Commands on page 234](#)
- [Monitor Commands on page 236](#)

Configuration Commands

- [Generic Commands on page 192](#)
- [Filter Log Commands on page 193](#)
- [Filter Policy Commands on page 196](#)
- [General Filter Entry Commands on page 200](#)
- [IP and MAC Filter Entry Commands on page 201](#)
- [IP and MAC Filter Match Criteria Commands on page 206](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>filter>ip-filter config>filter>log config>filter>ip-filter>entry config>filter>ipv6-filter config>filter>ipv6-filter>entry config>filter>mac-filter config>filter>mac-filter>entry
Description	<p>This command creates a text description for a configuration context to help identify the content in the configuration file.</p> <p>The no form of the command removes any description string from the context.</p>
Default	n/a
Parameters	<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, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>filter>log config>filter>log>summary
Description	<p>The shutdown command administratively disables the entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the no shutdown command.</p> <p>Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system-generated configuration files.</p> <p>The no form of the command puts an entity into the administratively enabled state.</p>
Default	no shutdown

Filter Log Commands

log

Syntax	log <i>log-id</i> [create] no log <i>log-id</i>
Context	config>filter
Description	<p>This command enables the context to create a filter log policy.</p> <p>The no form of the command deletes the filter log ID. The log cannot be deleted if there are filter entries configured to write to the log. All filter entry logging associations need to be removed before the log can be deleted.</p>

Special Cases

Filter log 101 — Filter log 101 is the default log and is automatically created by the system. Filter log 101 is always a memory filter log and cannot be changed to a syslog filter log. The log size defaults to 1000 entries. The number of entries and wrap-around behavior can be edited.

Default	log 101
Parameters	<i>log-id</i> — the filter log ID destination expressed as a decimal integer
Values	101 to 199

destination

Syntax	destination memory <i>num-entries</i> destination syslog <i>syslog-id</i> no destination
Context	config>filter>log
Description	<p>This command configures the destination for filter log entries for the specified filter log ID.</p> <p>Filter logs can be sent to either memory or an existing syslog server. If the filter log destination is memory, the maximum number of entries in the log must be specified.</p> <p>The no form of the command deletes the filter log association.</p>
Default	no destination

Parameters	<i>num-entries</i> — specifies that the destination of the filter log ID is a memory log. The <i>num-entries</i> value is the maximum number of entries in the filter log expressed as a decimal integer.
	Values 1 to 50000
	<i>syslog-id</i> — specifies that the destination of the filter log ID is a syslog server. The <i>syslog-id</i> parameter is the identifier of the syslog server.
	Values 1 to 10

summary

Syntax	summary
Context	config>filter>log
Description	This command enables the context to configure log summarization. These settings apply only if syslog is the log destination.

summary-crit

Syntax	summary-crit dst-addr summary-crit src-addr no summary-crit
Context	config>filter>log>summary
Description	<p>This command defines the key of the index of the mini-table. If key information is changed while summary is in the no-shutdown state, the filter summary mini-table is flushed and reconfigured with different key information. Log packets received during the reconfiguration time will be handled as if summary was not active.</p> <p>The no form of the command reverts to the default parameter.</p>
Default	dst-addr
Parameters	dst-addr — specifies that received log packets are summarized based on the destination IP address src-addr — specifies that received log packets are summarized based on the source IP address

wrap-around

Syntax	[no] wrap-around
Context	config>filter>log
Description	<p>This command configures a memory filter log to store log entries until full or to store the most recent log entries (circular buffer).</p> <p>Specifying wrap-around configures the memory filter log to store the most recent filter log entries (circular buffer). When the log is full, the oldest filter log entries are overwritten with new entries.</p> <p>The no form of the command configures the memory filter log to accept filter log entries until full. When the memory filter log is full, filter logging for the log filter ID ceases.</p>
Default	wrap-around

Filter Policy Commands

ip-filter

Syntax	ip-filter <i>filter-id</i> [create] no ip-filter <i>filter-id</i>
Context	config>filter
Description	<p>This command creates a configuration context for an IPv4 filter policy.</p> <p>IP filter policies specify either a forward or a drop action for packets based on the specified match criteria.</p> <p>The IP filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple network ports as long as the scope of the policy is template.</p> <p>Any changes made to the existing policy, using any of the subcommands, will be applied immediately to all network interfaces where this policy is applied.</p> <p>The no form of the command deletes the IP filter policy. A filter policy cannot be deleted until it is removed from all network interfaces where it is applied.</p>
Parameters	<i>filter-id</i> — the IP filter policy ID number
Values	1 to 65535
	create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

ipv6-filter

Syntax	ipv6-filter <i>ipv6-filter-id</i> [create] no ipv6-filter <i>ipv6-filter-id</i>
Context	config>filter
Description	<p>This command creates a configuration context for an IPv6 filter policy.</p> <p>IP filter policies specify either a forward or a drop action for packets based on the specified match criteria.</p> <p>The IP filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple network ports as long as the scope of the policy is template.</p>

Any changes made to the existing policy, using any of the subcommands, will be applied immediately to all network interfaces where this policy is applied.

The **no** form of the command deletes the IP filter policy. A filter policy cannot be deleted until it is removed from all network interfaces where it is applied.

Parameters *ipv6-filter-id* — the IPv6 filter policy ID number

Values 1 to 65535

create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the **create** keyword.

mac-filter

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

Context config>filter

Description This command enables the context for a MAC filter policy.

The MAC filter policy specifies either a forward or a drop action for packets based on the specified match criteria.

The MAC filter policy, sometimes referred to as an access control list, is a template that can be applied to multiple services as long as the **scope** of the policy is **template**.

A MAC filter policy cannot be applied to a network interface, a VPRN service, or an IES service.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied.

The **no** form of the command deletes the MAC filter policy. A filter policy cannot be deleted until it is removed from all SAPs where it is applied.

Parameters *filter-id* — the MAC filter policy ID number

Values 1 to 65535

create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the **create** keyword.

default-action

Syntax	default-action {drop forward}
Context	config>filter>ip-filter config>filter>ipv6-filter config>filter>mac-filter
Description	This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP or MAC filter entries of the filter.
Default	drop
Parameters	drop — specifies that all packets will be dropped unless there is a specific filter entry that causes the packet to be forwarded forward — specifies that all packets will be forwarded unless there is a specific filter entry that causes the packet to be dropped

renum

Syntax	renum <i>old-entry-id new-entry-id</i>
Context	config>filter>ip-filter config>filter>ipv6-filter config>filter>mac-filter
Description	This command renumbers existing IP or MAC filter entries to properly sequence filter entries. This may be required in some cases since the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.
Parameters	<i>old-entry-id</i> — the entry number of an existing entry Values 1 to 64 <i>new-entry-id</i> — the new entry number to be assigned to the old entry Values 1 to 64

scope

Syntax	scope {exclusive template} no scope
Context	config>filter>ip-filter config>filter>ipv6-filter config>filter>mac-filter
Description	<p>This command configures the filter policy scope as exclusive or template. If the scope of the policy is template and is applied to one or more network interfaces, the scope cannot be changed.</p> <p>The no form of the command sets the scope of the policy to the default of template.</p>
Default	template
Parameters	<p>exclusive — when the scope of a policy is defined as exclusive, the policy can only be applied to a single entity (network port). If an attempt is made to assign the policy to a second entity, an error message will result. If the policy is removed from the entity, it will become available for assignment to another entity.</p> <p>template — when the scope of a policy is defined as template, the policy can be applied to multiple network ports</p>

General Filter Entry Commands

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>filter>ip-filter config>filter>ipv6-filter config>filter>mac-filter
Description	<p>This command creates or edits an IPv4, IPv6, or MAC filter entry. Multiple entries can be created using unique entry-id numbers within the filter. The 7705 SAR implementation exits the filter on the first match found and executes the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.</p> <p>An entry might not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and hence will be rendered inactive.</p> <p>The no form of the command removes the specified entry from the IP or MAC filter. Entries removed from the IP or MAC filter are immediately removed from all SAPs, SDPs (mesh or spoke), or network ports where that filter is applied.</p>
Default	n/a
Parameters	<p><i>entry-id</i> — an entry-id uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given <i>entry-ids</i> in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.</p> <p>Values 1 to 64</p> <p>create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.</p>

IP and MAC Filter Entry Commands

action

Syntax	action {drop forward} no action
Context	config>filter>ip-filter>entry config>filter>ipv6-filter>entry config>filter>mac-filter>entry
Description	<p>This command specifies what action to take (drop or forward) if the packets match the entry criteria. The action keyword must be entered and a keyword specified in order for the entry to be active.</p> <p>Multiple action statements entered will overwrite previous action statements when defined.</p> <p>The no form of the command removes the specified action statement. The filter entry is considered incomplete and is rendered inactive without the action keyword.</p>
Default	n/a
Parameters	<p>drop — specifies that packets matching the entry criteria will be dropped</p> <p>forward — specifies that packets matching the entry criteria will be forwarded</p> <p>If neither drop nor forward is specified, the filter action is No-Op and the filter entry is inactive.</p>

log

Syntax	log <i>log-id</i> no log
Context	config>filter>ip-filter>entry config>filter>ipv6-filter>entry config>filter>mac-filter>entry
Description	<p>This command enables the context to enable filter logging for a filter entry and specifies the destination filter log ID.</p> <p>The filter log ID must exist before a filter entry can be enabled to use the filter log ID.</p> <p>The no form of the command disables logging for the filter entry.</p>
Default	no log
Parameters	<p><i>log-id</i> — the filter log ID destination expressed as a decimal integer</p> <p>Values 101 to 199</p>

match

Syntax	match [protocol <i>protocol-id</i>] no match
Context	config>filter>ip-filter>entry
Description	<p>This command enables the context to enter match criteria for the IPv4 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.</p> <p>If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.</p> <p>A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.</p> <p>The no form of the command removes the match criteria for the <i>entry-id</i>.</p>
Parameters	<p>protocol — the protocol keyword 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.</p> <p><i>protocol-id</i> — configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Common protocol numbers include ICMP(1), TCP(6), UDP(17). The no form of the command removes the protocol from the match criteria.</p> <p>Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary - DHB)</p> <p>keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp * — udp/tcp wildcard</p>

Protocol ID	Protocol	Description
1	icmp	Internet Control Message
2	igmp	Internet Group Management
4	ip	IP in IP (encapsulation)
6	tcp	Transmission Control
8	egp	Exterior Gateway Protocol
9	igp	Any private interior gateway
17	udp	User Datagram
27	rdp	Reliable Data Protocol
41	ipv6	IPv6
43	ipv6-route	Routing Header for IPv6

Protocol ID	Protocol	Description
45	idrp	Inter-Domain Routing Protocol
46	rsvp	Reservation Protocol
47	gre	General Routing Encapsulation
58	ipv6-icmp	ICMP for IPv6
59	ipv6-no-nxt	No Next Header for IPv6
60	ipv6-opts	Destination Options for IPv6
80	iso-ip	ISO Internet Protocol
88	eigrp	EIGRP
89	ospf-igp	OSPF/IGP
97	ether-ip	Ethernet-within-IP Encapsulation
98	encap	Encapsulation Header
102	pnni	PNNI over IP
103	pim	Protocol Independent Multicast
112	vrrp	Virtual Router Redundancy Protocol
115	l2tp	Layer Two Tunneling Protocol
118	stp	Schedule Transfer Protocol
123	ptp	Performance Transparency Protocol
124	isis	ISIS over IPv4
126	crtp	Combat Radio Transport Protocol
127	crudp	Combat Radio User Datagram



Note: PTP in the context of IP filters is defined as Performance Transparency Protocol. IP protocols can be used as IP filter match criteria; the match is made on the 8-bit protocol field in the IP header.

PTP in the context of SGT QoS is defined as Precision Timing Protocol and is an application in the 7705 SAR. The PTP application name is also used in areas such as event-control and logging. Precision Timing Protocol is defined in IEEE 1588-2008.

match

Syntax	match [next-header <i>next-header</i>] no match
Context	config>filter>ipv6-filter>entry
Description	<p>This command enables the context to enter match criteria for the IPv6 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.</p> <p>If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.</p> <p>A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.</p> <p>The no form of the command removes the match criteria for the <i>entry-id</i>.</p>
Parameters	<p><i>next-header</i> — the IPv6 next header to match. This parameter is similar to the protocol parameter used in IPv4 filter match criteria.</p> <p>Values [1 to 42 45 to 49 52 to 59 61 to 255] — (values can be expressed in decimal, hexadecimal, or binary - DHB)</p> <p>keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp * — udp/tcp wildcard</p>

match

Syntax	match frame-type {802dot3 802dot2-llc 802dot2-snap ethernet_II} no match
Context	config>filter>mac-filter>entry
Description	<p>This command creates the context for entering/editing match criteria for the filter entry and specifies an Ethernet frame type for the entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.</p> <p>If more than one match criterion (within one match statement) is configured, then all criteria must be satisfied (AND function) before the action associated with the match will be executed.</p> <p>A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.</p> <p>The no form of the command removes the match criteria for the <i>entry-id</i>.</p>
Default	frame-type 802dot3

Parameters

- frame-type** — configures an Ethernet frame type to be used for the MAC filter match criteria
- 802dot3** — specifies the frame type as Ethernet IEEE 802.3
- 802dot2-llc** — specifies the frame type as Ethernet IEEE 802.2 LLC
- 802dot2-snap** — specifies the frame type as Ethernet IEEE 802.2 SNAP
- ethernet_II** — specifies the frame type as Ethernet Type II

IP and MAC Filter Match Criteria Commands

dscp

Syntax	dscp <i>dscp-name</i> no dscp
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion. The no form of the command removes the DSCP match criterion.
Default	no dscp
Parameters	<i>dscp-name</i> — a DSCP name that has been previously mapped to a value using the dscp-name command. The DiffServ Code Point may only be specified by its name. Values be cp1 cp2 cp3 cp4 cp5 cp6 cp7 cs1 cp9 af11 cp11 af12 cp13 af13 cp15 cs2 cp17 af21 cp19 af22 cp21 af23 cp23 cs3 cp25 af31 cp27 af32 cp29 af33 cp31 cs4 cp33 af41 cp35 af42 cp37 af43 cp39 cs5 cp41 cp42 cp43 cp44 cp45 ef cp47 nc1 cp49 cp50 cp51 cp52 cp53 cp54 cp55 nc2 cp57 cp58 cp59 cp60 cp61 cp62 cp63

dst-ip

Syntax	dst-ip { <i>ip-address/mask</i> <i>ip-address netmask</i> } no dst-ip
Context	config>filter>ip-filter>entry>match
Description	This command configures a destination IPv4 address range to be used as an IP filter match criterion. To match on the destination IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used. The no form of the command removes the destination IP address match criterion.
Default	n/a
Parameters	<i>ip-address</i> — the IP prefix for the IP match criterion in dotted-decimal notation Values 0.0.0.0 to 255.255.255.255 <i>mask</i> — the subnet mask length expressed as a decimal integer Values 0 to 32

netmask — any mask expressed in dotted-decimal notation

Values 0.0.0.0 to 255.255.255.255

dst-ip

Syntax	dst-ip <i>ipv6-address/prefix-length</i> no dst-ip						
Context	config>filter>ipv6-filter>entry>match						
Description	<p>This command configures a destination IPv6 address range to be used as an IP filter match criterion.</p> <p>To match on the destination IP address, specify the address and prefix length; for example, 11::12/128.</p> <p>The no form of the command removes the destination IP address match criterion.</p>						
Default	n/a						
Parameters	<i>ipv6-address/prefix-length</i> — the IPv6 address on the interface						
	<table><tr><td>Values</td><td><i>ipv6-address</i></td><td>x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D</td></tr><tr><td></td><td><i>prefix-length</i></td><td>1 to 128</td></tr></table>	Values	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D		<i>prefix-length</i>	1 to 128
Values	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D					
	<i>prefix-length</i>	1 to 128					

dst-mac

Syntax	dst-mac <i>ieee-address</i> no dst-mac		
Context	config>filter>mac-filter>entry>match		
Description	<p>This command configures a destination MAC address to be used as a MAC filter match criterion.</p> <p>To match on the destination MAC address, specify the IEEE address.</p> <p>The no form of the command removes the destination MAC address match criterion.</p>		
Default	no dst-mac		
Parameters	<i>ieee-address</i> — the MAC address to be used as a match criterion		
	<table> <tr> <td>Values</td><td>xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit</td></tr> </table>	Values	xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit
Values	xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit		

dst-port

Syntax	dst-port { lt gt eq } <i>dst-port-number</i> dst-port range <i>start end</i> no dst-port
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	This command configures a destination TCP or UDP port number or port range for an IP filter match criterion. The no form of the command removes the destination port match criterion.
Default	n/a
Parameters	lt gt eq — use relative to <i>dst-port-number</i> for specifying the port number match criteria: lt specifies that all port numbers less than <i>dst-port-number</i> match gt specifies that all port numbers greater than <i>dst-port-number</i> match eq specifies that <i>dst-port-number</i> must be an exact match <i>dst-port-number</i> — the destination port number to be used as a match criteria expressed as a decimal integer Values 1 to 65535 <i>start end</i> — specifies an inclusive range of port numbers to be used as a match criteria. The destination port numbers <i>start</i> and <i>end</i> are expressed as decimal integers. Values 1 to 65535

etype

Syntax	etype <i>0x600...0xffff</i> no etype
Context	config>filter>mac-filter>entry>match
Description	This command configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion. The Ethernet type field is a 2 byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify IPv4 packets. The Ethernet type II frame Ethertype value to be used as a match criterion can be expressed as a hexadecimal (0x0600 to 0xFFFF) or a decimal (1536 to 65535) value. The Ethernet type field is used by the Ethernet version-II frames. The no form of the command removes the previously entered etype field as the match criteria.

Default **no etype**

fragment

Syntax	fragment {true false} no fragment
Context	config>filter>ip-filter>entry>match
Description	<p>This command configures fragmented or non-fragmented IP packets as an IP filter match criterion.</p> <p>The no form of the command removes the match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Default	false
Parameters	<p>true — configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.</p> <p>false — configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.</p>

icmp-code

Syntax	icmp-code <i>icmp-code</i> no icmp-code
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	<p>This command configures matching on an ICMP code field in the ICMP header of an IPv4 or IPv6 packet as a filter match criterion.</p> <p>This option is only meaningful if the protocol match criteria specifies ICMP (1).</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no icmp-code
Parameters	<p><i>icmp-code</i> — the ICMP code values that must be present to match</p> <p>Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary – DHB) keywords - none network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed dest-network-unknown dest-host-unknown</p>

icmp-type

Syntax	icmp-type <i>icmp-type</i> no icmp-type
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	<p>This command configures matching on the ICMP type field in the ICMP header of an IPv4 or IPv6 packet as a filter match criterion.</p> <p>This option is only meaningful if the protocol match criteria specifies ICMP (1).</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no icmp-type
Parameters	<i>icmp-type</i> — the ICMP type values that must be present to match
Values	0 to 255 (values can be expressed in decimal, hexadecimal, or binary – DHB) keywords - none echo-reply dest-unreachable echo-request time-exceeded parameter-problem

ip-option

Syntax	ip-option <i>ip-option-value</i> [<i>ip-option-mask</i>] no ip-option
Context	config>filter>ip-filter>entry>match
Description	<p>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.</p> <p>The option type octet contains 3 fields:</p> <ul style="list-style-type: none">• 1 bit copied flag (copy options in all fragments)• 2 bits option class• 5 bits option number <p>The no form of the command removes the match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Default	no ip-option
Parameters	<i>ip-option-value</i> — the 8-bit option type (can be entered using decimal, hexadecimal, or binary formats). The mask is applied as an AND to the option byte and the result is compared with the option value.

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

Values 0 to 255

ip-option-mask — specifies a range of option numbers to use as the match criteria

This 8-bit mask can be entered using decimal, hexadecimal, or binary formats:

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0x	0x14
Binary	0bBBBBBBBB	0b0010100

Default 255 (decimal) (exact match)

Values 0 to 255

multiple-option

Syntax	multiple-option {true false} no multiple-option
Context	config>filter>ip-filter>entry>match
Description	<p>This command configures matching packets that contain more than one option field in the IP header as an IP filter match criterion.</p> <p>The no form of the command removes the checking of the number of option fields in the IP header as a match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Default	no multiple-option
Parameters	<p>true — specifies matching on IP packets that contain more than one option field in the header</p> <p>false — specifies matching on IP packets that do not contain multiple option fields in the header</p>

option-present

Syntax	option-present {true false} no option-present
Context	config>filter>ip-filter>entry>match
Description	<p>This command configures matching packets that contain the option field or have an option field of 0 in the IP header as an IP filter match criterion.</p> <p>The no form of the command removes the checking of the option field in the IP header as a match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Parameters	<p>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 0 is considered as no option present.</p> <p>false — specifies matching on IP packets that do not have any option field present in the IP header (an option field of 0)</p>

src-ip

Syntax	src-ip {ip-address/mask ip-address netmask} no src-ip
Context	config>filter>ip-filter>entry>match
Description	<p>This command configures a source IPv4 address range to be used as an IP filter match criterion.</p> <p>To match on the source 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.</p> <p>The no form of the command removes the source IP address match criterion.</p>
Default	no src-ip
Parameters	<p><i>ip-address</i> — the IP prefix for the IP match criterion in dotted-decimal notation</p> <p>Values 0.0.0.0 to 255.255.255.255</p> <p><i>mask</i> — the subnet mask length expressed as a decimal integer</p> <p>Values 0 to 32</p> <p><i>netmask</i> — any mask expressed in dotted-decimal notation</p> <p>Values 0.0.0.0 to 255.255.255.255</p>

src-ip

Syntax	src-ip <i>ipv6-address/prefix-length</i> no src-ip		
Context	config>filter>ipv6-filter>entry>match		
Description	<p>This command configures a source IPv6 address range to be used as an IP filter match criterion.</p> <p>To match on the source IP address, specify the address and prefix length; for example, 11::12/128.</p> <p>The no form of the command removes the source IP address match criterion.</p>		
Default	n/a		
Parameters	<i>ipv6-address/prefix-length</i> — the IPv6 address on the interface		
	Values	<i>ipv6-address</i>	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
		<i>prefix-length</i>	1 to 128

src-mac

Syntax	src-mac <i>ieee-address</i> no src-mac		
Context	config>filter>mac-filter>entry>match		
Description	<p>This command configures a source MAC address to be used as a MAC filter match criterion.</p> <p>The no form of the command removes the source MAC address as the match criterion.</p>		
Default	no src-mac		
Parameters	<i>ieee-address</i> — the 48-bit IEEE MAC address to be used as a match criterion		
	Values	xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit	

src-port

Syntax	src-port { lt gt eq } <i>src-port-number</i> src-port range <i>start end</i> no src-port
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	<p>This command configures a source TCP or UDP port number or port range for an IP filter match criterion.</p> <p>The no form of the command removes the source port match criterion.</p>
Default	no src-port
Parameters	<p>lt gt eq — use relative to <i>src-port-number</i> for specifying the port number match criteria:</p> <ul style="list-style-type: none">lt specifies that all port numbers less than <i>src-port-number</i> matchgt specifies that all port numbers greater than <i>src-port-number</i> matcheq specifies that <i>src-port-number</i> must be an exact match <p><i>src-port-number</i> — the source port number to be used as a match criteria expressed as a decimal integer</p> <p>Values 1 to 65535</p> <p><i>start end</i> — specifies an inclusive range of port numbers to be used as a match criteria. The destination port numbers <i>start</i> and <i>end</i> are expressed as decimal integers.</p> <p>Values 1 to 65535</p>

tcp-ack

Syntax	tcp-ack { true false } no tcp-ack
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	<p>This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no tcp-ack
Parameters	<p>true — specifies matching on IP packets that have the ACK bit set in the control bits of the TCP header of an IP packet</p> <p>false — specifies matching on IP packets that do not have the ACK bit set in the control bits of the TCP header of the IP packet</p>

tcp-syn

Syntax	tcp-syn {true false} no tcp-syn
Context	config>filter>ip-filter>entry>match config>filter>ipv6-filter>entry>match
Description	<p>This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.</p> <p>The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP address.</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no tcp-syn
Parameters	<p>true — specifies matching on IP packets that have the SYN bit set in the control bits of the TCP header</p> <p>false — specifies matching on IP packets that do not have the SYN bit set in the control bits of the TCP header</p>

Show Commands

ip

Syntax	ip [<i>ip-filter-id</i> <i>ipv6-filter-id</i>] [entry <i>entry-id</i>] [association counters]
Context	show>filter
Description	This command displays IPv4 and IPv6 filter information.
Parameters	<p><i>ip-filter-id</i> <i>ipv6-filter-id</i> — displays detailed information for the specified filter ID and its filter entries</p> <p>Values 1 to 65535</p> <p><i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only</p> <p>Values 1 to 64</p> <p>association — appends information as to where the filter policy ID is applied to the detailed filter policy ID output</p> <p>counters — displays counter information for the specified filter ID</p>
Output	<p>The following outputs are examples of IP filter information:</p> <ul style="list-style-type: none">• IP filter information (Sample Output, Table 30)• IP filter information with filter ID specified (Sample Output, Table 31)• IP filter associations (Sample Output, Table 32)• IP filter counters (Sample Output, Table 33)

Sample Output

```

*A-ALU-1# show filter ip
=====
IP Filters
=====
Filter-Id Scope    Applied Description
-----
1           Template Yes
3           Template Yes
6           Template Yes
10          Template No
11          Template No
-----
Num IP filters: 5
=====
*A-ALU-1#

*A-ALU-1# show filter ipv6
=====
IPv6 Filters
=====
Filter-Id Scope    Applied Description
-----
1           Template No
-----
Num IP filters: 1
=====
*A-ALU-1#

```

Table 30: Show Filter Output Fields

Label	Description
Filter Id	The IP filter ID
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Description	The IP filter policy description

Sample Output

```
*A-ALU-1# show filter ip 3
=====
IP Filter
=====
Filter Id      : 3                      Applied      : Yes
Scope         : Template                Def. Action   : Drop
Entries       : 1
-----
Filter Match Criteria : IP
-----
Entry         : 10
Description    : this is a test ip-filter entry
Log Id        : n/a
Src. IP       : 10.1.1.1/24             Src. Port     : None
Dest. IP      : 0.0.0.0/0               Dest. Port    : None
Protocol      : Undefined               Dscp         : Undefined
ICMP Type     : Undefined               ICMP Code     : Undefined
Fragment      : Off                    Option-present : Off
IP-Option     : 0/0                    Multiple Option: Off
TCP-syn       : Off                    TCP-ack       : Off
Match action  : Drop
Ing. Matches  : 0 pkts
Egr. Matches  : 0 pkts

=====
*A-ALU-1#

*A-ALU-1# show filter ipv6 1
=====
IPv6 Filter
=====
Filter Id      : 1                      Applied      : No
Scope         : Template                Def. Action   : Drop
Entries       : 1
Description    : (Not Specified)
-----
Filter Match Criteria : IPv6
-----
Entry         : 1 (Inactive)
Description    : (Not Specified)
Log Id        : n/a
Src. IP       : ::/0                   Src. Port     : None
Dest. IP      : ::/0                   Dest. Port    : None
Next Header   : Undefined              Dscp         : Undefined
ICMP Type     : Undefined               ICMP Code     : Undefined
TCP-syn       : Off                    TCP-ack       : Off
Match action  : Drop
Ing. Matches  : 0 pkts
Egr. Matches  : 0 pkts

=====
*A-ALU-1#
```

Table 31: Show Filter Output Fields (Filter ID Specified)

Label	Description
Filter Id	The IP filter policy ID
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Entries	The number of entries configured in this filter ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Match Criteria	IP — the filter is an IPv4 filter policy
	IPv6 — the filter is an IPv6 filter policy
Entry	The filter entry ID. If the filter entry ID indicates that the entry is Inactive, the filter entry is incomplete as no action has been specified.
Description	The IP filter policy description
Src. IP	The source IP address and prefix length match criterion
Dest. IP	The destination IP address and prefix length match criterion
Protocol	The protocol ID for the match criteria. Undefined indicates no protocol specified. (IPv4 filters only)
Next Header	The next header ID for the match criteria. Undefined indicates no next header is specified. (IPv6 filters only)
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type is specified.
Fragment (IPv4 filters only)	Off — configures a match on all unfragmented packets
	On — configures a match on all fragmented packets
IP-Option	Specifies matching packets with a specific IP option or range of IP options in the IP header for IP filter match criteria (IPv4 filters only)
TCP-syn	Off — the SYN bit is disabled
	On — the SYN bit is set

Table 31: Show Filter Output Fields (Filter ID Specified) (Continued)

Label	Description
Match action	Default — the filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates that the entry is <i>Inactive</i> , the filter entry is incomplete as no action was specified.
	Drop — drop packets matching the filter entry
	Forward — forward packets matching the filter entry
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Src. Port	The source TCP or UDP port number or port range
Dest. Port	The destination TCP or UDP port number or port range
Dscp	The DSCP name
ICMP Code	The ICMP code field in the ICMP header of an IP packet
Option-present (IPv4 filters only)	Off — does not search for packets that contain the option field or have an option field of zero
	On — matches packets that contain the option field or have an option field of zero
Multiple Option (IPv4 filters only)	Off — the option fields are not checked
	On — packets containing one or more option fields in the IP header will be used as IP filter match criteria
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet

Sample Output

```

*A-ALU-49# show filter ip 1 associations
=====
IP Filter
=====
Filter Id      : 1                      Applied      : Yes
Scope         : Template                Def. Action   : Drop
Entries       : 1
-----
Filter Association : IP
-----
=====
Filter Match Criteria : IP
-----
Entry         : 10
Log Id        : n/a
Src. IP       : 10.1.1.1/24              Src. Port     : None
Dest. IP      : 0.0.0.0/0                Dest. Port    : None
Protocol      : 2                        Dscp          : Undefined
ICMP Type     : Undefined                ICMP Code     : Undefined
Fragment      : Off                      Option-present : Off
Sampling      : Off                      Int. Sampling  : On
IP-Option     : 0/0                      Multiple Option: Off
TCP-syn       : Off                      TCP-ack       : Off
Match action  : Drop
Ing. Matches  : 0                        Egr. Matches  : 0
=====
*A-ALU-49#

*A-ALU-49# show filter ip 1 associations
=====
IPv6 Filter
=====
Filter Id      : 1                      Applied      : No
Scope         : Template                Def. Action   : Drop
Entries       : 1
Description    : (Not Specified)
-----
Filter Association : IPv6
-----
No Match Found
=====
*A-ALU-49#

```

Table 32: Show Filter Associations Output Fields

Label	Description
Filter Id	The IP filter policy ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries configured in this filter ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Association	IP or IPv6
Entry	The filter entry ID. If the filter entry ID indicates that the entry is Inactive, the filter entry is incomplete as no action was specified.
Src. IP	The source IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Dest. IP	The destination IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Protocol	The protocol ID for the match criteria. Undefined indicates no protocol specified. (IPv4 filters only)
Next Header	The next header ID for the match criteria. Undefined indicates no next header is specified. (IPv6 filters only)
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.
Fragment (IPv4 filters only)	Off — configures a match on all unfragmented packets
	On — configures a match on all fragmented packets
TCP-syn	Off — the SYN bit is disabled
	On — the SYN bit is set
Match action	Default — the filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete (no action was specified).
	Drop — drop packets matching the filter entry
	Forward — forward packets matching the filter entry

Table 32: Show Filter Associations Output Fields (Continued)

Label	Description
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Src. Port	The source TCP or UDP port number or port range
Dest. Port	The destination TCP or UDP port number or port range
Dscp	The DSCP name
ICMP Code	The ICMP code field in the ICMP header of an IP packet
Option-present (IPv4 filters only)	Off — does not search for packets that contain the option field or have an option field of zero
	On — matches packets that contain the option field or have an option field of zero
Multiple Option (IPv4 filters only)	Off — the option fields are not checked
	On — packets containing one or more option fields in the IP header will be used as IP filter match criteria
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet

Sample Output

```
*A-ALU-1# show filter ip 3 counters
=====
IP Filter : 100
=====
Filter Id   : 3                               Applied      : Yes
Scope      : Template                         Def. Action   : Drop
Entries    : Not Available
-----
Filter Match Criteria : IP
-----
Entry       : 10
Ing. Matches: 749                               Egr. Matches  : 0

Entry       : 200
Ing. Matches: 0                               Egr. Matches  : 0

=====
*A-ALU-1#

*A-ALU-1# show filter ipv6 1 counters
=====
IPv6 Filter
=====
Filter Id   : 1                               Applied      : No
Scope      : Template                         Def. Action   : Drop
Entries    : 1
Description : (Not Specified)
-----
Filter Match Criteria : IPv6
-----
Entry       : 1 (Inactive)
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

=====
*A-ALU-1#
```


Table 33: Show Filter Counters Output Fields

Label	Description
Filter Id	The IP filter policy ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries configured in this filter ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Match Criteria	IP — indicates the filter is an IPv4 filter policy
	IPv6 — indicates the filter is an IPv6 filter policy
Entry	The filter entry ID. If the filter entry ID indicates the entry is (Inactive), the filter entry is incomplete as no action has been specified.
Ing. Matches	The number of ingress filter matches/hits for the filter entry

log

Syntax **log** [bindings]
log *log-id* [*match string*]

Context show>filter

Description This command displays filter log information. When a filter **log** command is used with a MAC filter and a packet is matched, the log entry is different from an IP filter entry. For a MAC filter, the source and destination IP address of incoming packets are not included in the log.

Parameters **bindings** — displays the number of filter logs currently available
log-id — the filter log ID destination expressed as a decimal integer

Values 101 to 199

string — specifies to display the log entries starting from the first occurrence of the specified string

Values up to 32 characters

Output The following outputs are examples of filter log information:

- filter log information ([Sample Output, Table 34](#))
- filter log bindings ([Sample Output, Table 35](#))

Sample Output

```

*A-ALU-1# show filter log

=====
Filter Logs
=====
Log-Id Dest.  Id/Entries Enabled Description
-----
101      Memory 1000      Yes      Default filter log
          Wrap: Enabled

1 Entries Found
=====
*A-ALU-1#

*A-ALU-1# show filter log 101

=====
Filter Log
=====
Admin state : Enabled
Description : Default filter log
Destination : Memory
Wrap        : Enabled
-----
Maximum entries configured : 1000
Number of entries logged   : 0
=====

```

Table 34: Show Filter Log Output Fields

Label	Description
Log-Id	The filter log ID
Dest./Destination	The destination of the filter log: memory or syslog
Id/Entries	The number of entries configured for this filter log
Enabled	Indicates whether the log is administratively enabled
Admin State	The administrative state of the log: enabled or disabled
Description	The description string configured for the filter log
Wrap	Indicates whether the wrap-around function (circular buffer) is enabled
Maximum entries configured	The maximum number of entries allowed in this filter log
Number of entries logged	The number of entries in this filter log

Sample Output

```
*A-ALU-1# show filter log bindings
```

```
=====
Filter Log Bindings
=====
Total Log Instances (Allowed)      : 2047
Total Log Instances (In Use)      : 1
Total Log Bindings                : 1

-----
Type  FilterId EntryId  Log    Instantiated
-----
Cpm           1        2   101           Yes
-----
=====
```

Table 35: Show Filter Log Bindings

Label	Description
Total Log Instances (Allowed)	The maximum allowed instances of filter logs allowed on the system
Total Log Instances (In Use)	The instances of filter logs presently existing on the system
Total Log Bindings	The count of the filter log bindings presently existing on the system
Type	The type of filter: CPM, IP, or MAC
FilterID	The unique identifier of the filter
EntryID	The unique identifier of an entry in the filter table
Log	The filter log identifier
Instantiated	Specifies if the filter log for this filter entry has been enabled

mac

Syntax	mac { <i>mac-filter-id</i> [entry <i>entry-id</i>] [associations counters]}
Context	show>filter
Description	This command displays MAC filter information.
Parameters	<p><i>mac-filter-id</i> — displays detailed information for the specified filter ID and its filter entries</p> <p>Values 1 to 65535</p> <p>entry <i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID</p> <p>Values 1 to 65535</p> <p>associations — displays information on where the filter policy ID is applied to the detailed filter policy ID output</p> <p>counters — displays counter information for the specified filter ID</p>
Output	<p>The following outputs are examples of MAC filter information:</p> <ul style="list-style-type: none"> no parameters specified (Sample Output, Table 36) <i>mac-filter-id</i> specified (Sample Output, Table 37) associations specified (Sample Output, Table 38) counters specified (Sample Output, Table 39)

Sample Output

When no parameters are specified, a brief listing of MAC filters is produced.

```
*A-ALU-1>show>filter# mac

=====
Mac Filters                                     Total:      3
=====
Filter-Id Scope      Applied Description
-----
11          Template No
232         Template Yes      filter-west
5000        Template No
-----
Num MAC filters: 3
=====
*A-ALU-1#
```

Table 36: Show Filter MAC (No Filter- D Specified)

Label	Description
Filter-Id	The MAC filter ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Description	The MAC filter policy description

Sample Output

When the filter ID is specified, detailed filter information for the filter ID and its entries is displayed.

```
*A-ALU-1# show filter# mac 5000

=====
Mac Filter
=====
Filter Id   : 5000                               Applied      : No
Scope      : Template                           Def. Action   : Drop
Entries     : 1
Description : (Not Specified)
-----
Filter Match Criteria : Mac
-----
Entry       : 5000 (Inactive)                     FrameType     : Ethernet
Description : (Not Specified)
Log Id      : n/a
Src Mac     : ff:ff:ff:ff:ff:ff ff:ff:ff:ff:ff:ff
Dest Mac    :
Dot1p       : Undefined                           Ethertype     : Undefined
DSAP        : Undefined                           SSAP          : Undefined
Snap-pid    : Undefined                           ESnap-oui-zero : Undefined
Match action: Drop
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

=====
*A-ALU-1#
```

Table 37: Show Filter MAC (Filter ID Specified)

Label	Description
MAC Filter	
Filter Id	The MAC filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop —
Entries	The number of entries in the filter policy
Description	The MAC filter policy description
Filter Match Criteria: Mac	
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified
FrameType	Ethernet — the entry ID match frame type is Ethernet IEEE 802.3
	Ethernet II — the entry ID match frame type is Ethernet Type II.
Description	The filter entry description
Log Id	The filter log identifier
Src Mac	The source MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion is specified for the filter entry
Dest Mac	The destination MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion is specified for the filter entry
Dot1p	The IEEE 802.1p value for the match criterion. Undefined indicates that no value is specified
Ethertype	The Ethertype value match criterion

Table 37: Show Filter MAC (Filter ID Specified) (Continued)

Label	Description
DSAP	The DSAP value match criterion. Undefined indicates that no value is specified
SSAP	The SSAP value match criterion. Undefined indicates that no value is specified
Snap-pid	The Ethernet SNAP PID value match criterion. Undefined indicates that no value is specified
Esnap-oui-zero	Non-Zero — filter entry matches a non-zero value for the Ethernet SNAP OUI
	Zero — filter entry matches a zero value for the Ethernet SNAP OUI
	Undefined — no Ethernet SNAP OUI value is specified
Match action	Default — the filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified
	Drop — packets matching the filter entry criteria will be dropped —
	Forward — packets matching the filter entry criteria are forwarded
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

Sample Output

```

*A-ALU-1# show filter# mac 11 associations
=====
Mac Filter
=====
Filter Id   : 11                               Applied      : No
Scope      : Template                         Def. Action   : Drop
Entries    : 1
Description : (Not Specified)
-----
Filter Association : Mac
-----
No Match Found
=====
*A-ALU-1#

```

Table 38: Show Filter MAC Associations

Label	Description
Filter Id	The IP filter ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries in the filter
Description	The MAC filter policy description
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Association	The type of filter association

Sample Output

```
*A-ALU-1# show filter# mac 11 counters
```

```
=====
Mac Filter
=====
Filter Id   : 11                      Applied      : No
Scope      : Template                Def. Action   : Drop
Entries    : 1
Description : (Not Specified)
-----
Filter Match Criteria : Mac
-----
Entry       : 11 (Inactive)          FrameType    : Ethernet II
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts
=====
*A-ALU-1#
```


Table 39: Show Filter MAC Counters

Label	Description
Filter Id	The IP filter ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries in the filter
Description	The MAC filter policy description
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Match Criteria: Mac	
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
FrameType	Ethernet — the entry ID match frame type is Ethernet IEEE 802.3
	Ethernet II — the entry ID match frame type is Ethernet Type II
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

Clear Commands

ip

Syntax	ip <i>ip-filter-id</i> [entry <i>entry-id</i>] [ingress egress]
Context	clear>filter
Description	<p>This command clears the counters associated with the IPv4 filter policy.</p> <p>By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.</p>
Default	clears all counters associated with the IPv4 filter policy entries
Parameters	<p><i>ip-filter-id</i> — the IPv4 filter policy ID</p> <p>Values 1 to 65535</p> <p><i>entry-id</i> — only the counters associated with the specified filter policy entry will be cleared</p> <p>Values 1 to 64</p> <p>ingress — only the ingress counters will be cleared</p> <p>egress — only the egress counters will be cleared</p>

ipv6

Syntax	ipv6 <i>ipv6-filter-id</i> [entry <i>entry-id</i>] [ingress egress]
Context	clear>filter
Description	<p>This command clears the counters associated with the IPv6 filter policy.</p> <p>By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.</p>
Default	clears all counters associated with the IPv6 filter policy entries
Parameters	<p><i>ipv6-filter-id</i> — the IPv6 filter policy ID</p> <p>Values 1 to 65535</p> <p><i>entry-id</i> — only the counters associated with the specified filter policy entry will be cleared</p> <p>Values 1 to 64</p> <p>ingress — only the ingress counters will be cleared</p> <p>egress — only the egress counters will be cleared</p>

log

Syntax	log <i>log-id</i>
Context	clear>filter
Description	This command clears the entries associated with the specified filter log. The clear command applies only to logs whose destination is to memory.
Parameters	<i>log-id</i> — the filter log ID destination expressed as a decimal integer
Values	101 to 199

mac

Syntax	mac <i>mac-filter-id</i> [entry <i>entry-id</i>] [ingress egress]
Context	clear>filter
Description	<p>This command clears the counters associated with the MAC filter policy.</p> <p>By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.</p>
Default	clears all counters associated with the MAC filter policy entries
Parameters	<p><i>mac-filter-id</i> — the MAC filter policy ID</p> <p>Values 1 to 65535</p> <p><i>entry-id</i> — only the counters associated with the specified filter policy entry will be cleared</p> <p>Values 1 to 64</p> <p>ingress — only the ingress counters will be cleared</p> <p>egress — only the egress counters will be cleared (currently not supported on the 7705 SAR)</p>

Monitor Commands

filter

Syntax	filter ip <i>ip-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor
Description	This command monitors the counters associated with the IPv4 filter policy.
Parameters	<i>ip-filter-id</i> — the IPv4 filter policy ID Values 1 to 65535 <i>entry-id</i> — only the counters associated with the specified filter policy entry will be monitored Values 1 to 64 <i>seconds</i> — configures the interval for each display in seconds Values 3 to 60 Default 5 <i>repeat</i> — configures how many times the command is repeated Values 1 to 999 Default 10 absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics. rate — the rate per second for each statistic is displayed instead of the delta

filter

Syntax	filter ipv6 <i>ipv6-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor
Description	This command monitors the counters associated with the IPv6 filter policy.
Parameters	<i>ipv6-filter-id</i> — the IPv6 filter policy ID Values 1 to 65535 <i>entry-id</i> — only the counters associated with the specified filter policy entry will be monitored Values 1 to 64

seconds — configures the interval for each display in seconds

Values 3 to 60

Default 5

repeat — configures how many times the command is repeated

Values 1 to 999

Default 10

absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.

rate — the rate per second for each statistic is displayed instead of the delta

filter

Syntax	filter mac <i>mac-filter-id</i> entry <i>entry-id</i> [interval <i>seconds</i>] [repeat <i>repeat</i>] [absolute rate]
Context	monitor
Description	This command monitors the counters associated with the MAC filter policy.
Parameters	<p><i>mac-filter-id</i> — the MAC filter policy ID</p> <p>Values 1 to 65535</p> <p><i>entry-id</i> — only the counters associated with the specified filter policy entry will be monitored</p> <p>Values 1 to 64</p> <p><i>seconds</i> — configures the interval for each display in seconds</p> <p>Values 3 to 60</p> <p>Default 5</p> <p><i>repeat</i> — configures how many times the command is repeated</p> <p>Values 1 to 999</p> <p>Default 10</p> <p>absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.</p> <p>rate — the rate per second for each statistic is displayed instead of the delta</p>

Route Policies

In This Chapter

This chapter provides information about configuring route policies.

Topics in this chapter include:

- [Configuring Route Policies on page 240](#)
 - [Routing Policy and MPLS on page 240](#)
 - [Policy Statements on page 241](#)
 - [Default Action Behavior on page 241](#)
 - [Denied IP Prefixes on page 242](#)
 - [Controlling Route Flapping on page 242](#)
 - [Regular Expressions on page 244](#)
 - [BGP and OSPF Route Policy Support on page 248](#)
 - [BGP Route Policies on page 249](#)
 - [Readvertised Route Policies on page 249](#)
 - [When to Use Route Policies on page 249](#)
- [Route Policy Configuration Process Overview on page 250](#)
- [Configuration Notes on page 251](#)
- [Configuring Route Policies with CLI on page 253](#)
- [Route Policy Command Reference on page 275](#)

Configuring Route Policies

Route policies are used to manage the label database for MPLS and to control entries to the routing table for dynamic routing.

See [Routing Policy and MPLS](#) for information on how routing policies can be used to manage the MPLS label database.

For routing, the 7705 SAR supports two databases to store routes. The routing database (RIB) is composed of the routing information learned by the routing protocols, including static routes. The forwarding database (FIB) is composed of the routes actually used to forward traffic through a router. In addition, link-state databases are maintained by interior gateway protocols (IGPs) such as OSPF and IS-IS. Refer to the 7705 SAR OS Routing Protocols Guide for information on OSPF and IS-IS.

Routing protocols calculate the best route to each destination and place these routes in the forwarding table. The routes in the forwarding table are used to forward IP packets to neighbors.

As an example, operators can configure a routing policy that will not place routes associated with a specific origin in the routing table. These routes will not be used to forward data packets and these routes are not advertised by the routing protocol to neighbors.

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Careful planning is essential to implement route policies that can affect the flow of routing information throughout the network. Before configuring and applying a route policy, operators should develop an overall plan and strategy to accomplish their intended routing actions.

There are no default route policies. Each policy must be created explicitly and applied. Policy parameters are modifiable.

Routing Policy and MPLS

Route policies can be used to manage the label database for MPLS.

When used to manage the label database, route policies can be configured to determine which labels should be learned or advertised; for example, labels from a specified neighbor can be added to the label information base (LIB), while labels advertised by certain other neighbors can be discarded. Label learning of MPLS packets and, as a result, how the MPLS packets are forwarded, are based on the defined policies, if there are any. If no route policies are defined, all advertised labels received from neighbors are learned and placed in the LIB.

Refer to the 7705 SAR OS MPLS Guide for more information on how routing policies can be used as LDP import policies to control the label bindings an LSR accepts from its peers.

Policy Statements

Route policies contain policy statements containing ordered entries that contain match conditions and actions that the user specifies. The entries should be sequenced from the most explicit to the least explicit. Packet forwarding and routing can be implemented according to defined policies. Policy-based routing allows the user to dictate where traffic can be routed, through specific paths, or whether to forward or drop the traffic. Route policies can match a given route policy entry and continue searching for other matches within either the same route policy or the next route policy.

The process can stop when the first complete match is found and the router executes the action defined in the entry, either to accept or reject packets that match the criteria or proceed to the next entry or the next policy. Matching criteria can be based on source, destination, or particular properties of a route. Route policies can be constructed to support multiple stages to the evaluation and setting various route attributes.

Other matching conditions can be provided by specifying criteria such as:

- autonomous system (AS) path policy options — a combination of AS numbers and regular expression operators
- community list — a group sharing a common property
- prefix list — a named list of prefixes
- to and from criteria — a route's destination and source

Default Action Behavior

The default action specifies how packets are to be processed when a policy related to the route is not explicitly configured. The following default actions are applied in the event that:

- a route policy does not specify a matching condition; all the routes being compared with the route policy are considered to be matches
- a match does not occur when the last entry in the last policy is evaluated
- if no default action is specified, the default behavior of the protocol controls whether the routes match or not

If a default action is defined for one or more of the configured route policies, then the default action is handled as follows.

- The default action can be set to all available action states, including accept, reject, next-entry, and next-policy.
- If the action states accept or reject, the policy evaluation terminates and the appropriate result is returned.

- If a default action is defined and no matches occurred with the entries in the policy, the default action is used.
- If a default action is defined and one or more matches occurred with the entries of the policy, the default action is not used.

Denied IP Prefixes

The following IP address prefixes are not allowed by the routing protocols and the Route Table Manager and are not be populated within the forwarding table:

- 0.0.0.0/8 or longer
- 127.0.0.0/8 or longer
- 224.0.0.0/4 or longer
- 240.0.0.0/4 or longer

Any other prefixes that need to be filtered can be filtered explicitly using route policies.

Controlling Route Flapping

Route flapping is defined as recurring changes of an advertised route between nodes. That is, the advertised route alternates (flaps) back and forth between two paths. This is typically caused by network problems that cause intermittent route failures. Route flap is defined in RFC 2439.

Route damping is a controlled acceptance of unstable routes from BGP peers so that any ripple effect caused by route flapping across BGP AS border routers is minimized. The rationale is to delay the use of unstable routes (flapping routes) to forward data and advertisements until the route stabilizes.

The Alcatel-Lucent implementation of route damping is based on the following parameters:

- Figure of Merit — a route is assigned a Figure of Merit (FoM), which is proportional to the frequency of flaps. The FoM algorithm can characterize a route's behavior over a period of time. See [Damping](#) for more information on FoM and damping.
- route flap — a route flap is not limited to the withdrawn route. It also applies to any change in the AS path or the next hop of a reachable route. A change in AS path or next hop indicates that the intermediate AS or the route-advertising peer is not suppressing flapping routes at the source or during the propagation. Even if the route is accepted as a stable route, the data packets destined for the route could experience unstable routing due to the unstable AS path or next hop.

- suppress threshold — when the configured suppress threshold is exceeded, the route is suppressed and not advertised to other peers. The state of the route is considered to be down from the perspective of the routing protocol.
- reuse threshold — when the FoM value falls below the configured reuse threshold and the route is still reachable, the route is advertised to other peers. The FoM value decays exponentially after a route is suppressed.

The two events that could trigger the route flapping algorithm are:

- route flapping — if a route flap is detected within a configured maximum route flap history time, the route's FoM is initialized and the route is marked as a potentially unstable route. Every time a route flaps, the FoM is increased and the route is suppressed if the FoM crosses the suppress threshold.
- route reuse timer trigger — a suppressed route's FoM decays exponentially. When it crosses the reuse threshold, the route is eligible for advertisement if it is still reachable.

If the route continues to flap, the FoM, with respect to time scale, looks like a sawtooth waveform with the exponential rise and decay of FoM. To control flapping, the following parameters can be configured:

- half-life — the half-life value is the time, expressed in minutes, required for a route to remain stable in order for one half of the FoM value to be reduced. For example, if the half-life value is 6 (min) and the route remains stable for 6 min, then the new FoM value is 3. After another 6 min passes and the route remains stable, the new FoM value is 1.5.
- max-suppress — the maximum suppression time, expressed in minutes, is the maximum amount of time that a route can remain suppressed
- suppress — if the FoM value exceeds the configured integer value, the route is suppressed for use or inclusion in advertisements
- reuse — if the suppress value falls below the configured reuse value, then the route can be reused

Regular Expressions

The ability to perform a filter match in the AS-PATH is supported. This feature allows customers to configure match criteria for specific sequences within the AS path so that they can be filtered out before cluttering the service provider's routing information base (RIB).

The 7705 SAR OS uses regular expression strings to specify match criteria for:

- an AS path string; for example, "100 200 300"
- a community string; for example, "100:200", where 100 is the AS number and 200 is the community-value

A regular expression is expressed as a combination of terms and operators. Regular expressions should always be enclosed in quotes.

Terms

A term for an AS path regular expression is:

1. an elementary term; for example, an AS number "200"
2. a range term composed of two elementary terms separated by the "-" character, such as "200-300"
3. the "." dot wild-card character, which matches any elementary term
4. a regular expression enclosed in parenthesis "("
5. a regular expression enclosed in square brackets used to specify a set of choices of elementary or range terms; for example, [100-300 400] matches any AS number between 100 and 300 or the AS number 400

A term for a community string regular expression is a string that is evaluated character by character and is composed of:

1. an elementary term, which for a community string is any single digit, such as "4"
2. a range term composed of two elementary terms separated by the "-" character, such as "2-3"
3. a colon ":" to delimit the AS number from the community value
4. the "." dot wild-card character, which matches any elementary term or ":"
5. a regular expression enclosed in parenthesis "("
6. a regular expression enclosed in square brackets, which is used to specify a set of choices of elementary or range terms; for example, [1-3 7] matches any single digit between 1 and 3 or the digit 7

Operators

The regular expression operators are listed in [Table 40](#).

Table 40: Regular Expression Operators

Operator	Description
	Matches the term on alternate sides of the pipe
*	Matches multiple occurrences of the term
?	Matches 0 or 1 occurrence of the term
+	Matches 1 or more occurrence of the term
()	Used to parenthesize so a regular expression is considered as one term
[]	Used to demarcate a set of elementary or range terms
-	Used between the start and end of a range
{ <i>m,n</i> }	Matches at least <i>m</i> and at most <i>n</i> repetitions of the term
{ <i>m</i> }	Matches exactly <i>m</i> repetitions of the term
{ <i>m</i> ,}	Matches <i>m</i> or more repetitions of the term
^	Matches the beginning of the string — only allowed for communities
\$	Matches the end of the string — only allowed for communities
\	An escape character to indicate that the following character is a match criteria and not a grouping delimiter

Examples of AS path and community string regular expressions are listed in [Table 41](#).

Table 41: AS Path and Community Regular Expression Examples

AS Path to Match Criteria	Regular Expression	Examples of Matches
Null AS path	<code>null (1)</code>	Null AS path
AS path is 11	<code>11</code>	11
AS path is 11 22 33	<code>11 22 33</code>	11 22 33
Zero or more occurrences of AS number 11	<code>11*</code>	Null AS path 11 11 11 11 11 11 11 ... 11

Table 41: AS Path and Community Regular Expression Examples (Continued)

AS Path to Match Criteria	Regular Expression	Examples of Matches
Path of any length that begins with AS numbers 11, 22, 33	11 22 33 .*	11 22 33 11 22 33 400 500 600
Path of any length that ends with AS numbers 44, 55, 66	.* 44 55 66	44 55 66 100 44 55 66 100 200 44 55 66 100 200 300 44 55 66 100 200 300 ... 44 55 66
One occurrence of the AS numbers 100 and 200, followed by one or more occurrences of the number 33	100 200 33+	100 200 33 100 200 33 33 100 200 33 33 33 100 200 33 33 33 ... 33
One or more occurrences of AS number 11, followed by one or more occurrences of AS number 22, followed by one or more occurrences of AS number 33	11+ 22+ 33+	11 22 33 11 11 22 33 11 11 22 22 33 11 11 22 22 33 33 11 ... 11 22 ... 22 33 ...33
Path whose second AS number must be 11 or 22	(. 11) (. 22) .* or . (11 22) .*	100 11 200 22 300 400 ...
Path of length one or two whose second AS number might be 11 or 22	. (11 22)?	100 200 11 300 22
Path whose first AS number is 100 and second AS number is either 11 or 22	100 (11 22) .*	100 11 100 22 200 300
AS path 11, 22, or 33	[11 22 33]	11 22 33
Range of AS numbers to match a single AS number	10-14	10 or 11 or 12 or 13 or 14
	[10-12]*	Null AS path 10 or 11 or 12 10 10 or 10 11 or 10 12 11 10 or 11 11 or 11 12 12 10 or 12 11 or 12 12 ...
Zero or one occurrence of AS number 11	11? or 11{0,1}	Null AS path 11

Table 41: AS Path and Community Regular Expression Examples (Continued)

AS Path to Match Criteria	Regular Expression	Examples of Matches
One through four occurrences of AS number 11	11{1,4}	11 11 11 11 11 11 11 11 11 11
One through four occurrences of AS number 11 followed by one occurrence of AS number 22	11{1,4} 22	11 22 11 11 22 11 11 11 22 11 11 11 11 22
Path of any length, except nonexistent, whose second AS number can be anything, including nonexistent	. .* or . .{0,}	100 100 200 11 22 33 44 55
AS number is 100 and community value is 200	^100:200\$	100:200
AS number is 11 or 22 and community value is any number	^((11) (22)):(.*)\$	11:100 22:100 11:200 ...
AS number is 11 and community value is any number that starts with 1	^11:(1.*)\$	11:1 11:100 11:1100
AS number is any number and community value is any number that ends with 1, 2, or 3	^(.*):(.*[1-3])\$	11:1 100:2002 333:55553 ...
AS number is 11 or 22 and community value is any number that starts with 3 and ends with 4, 5 or 9	^((11) (22)):(3.*[459])\$	11:34 22:3335 11:3777779 ...
AS number is 11 or 22 and community value ends in 33 or 44	[^((11 22)):(.*((33) (44)))\$	11:33 22:99944 22:555533 ...
Note: 1. The null keyword matches an empty AS path.		

BGP and OSPF Route Policy Support

BGP and OSPF require route policy support. Figure 5 and Figure 6 show how route policies are evaluated in each protocol. Figure 5 depicts BGP support, which applies a route policy as an internal part of the BGP route selection process. Figure 6 depicts OSPF support, which applies routing policies at the edge of the protocol, in order to control only the routes that are announced to or accepted from the Routing Table Manager (RTM).

Figure 5: BGP Route Policy Diagram

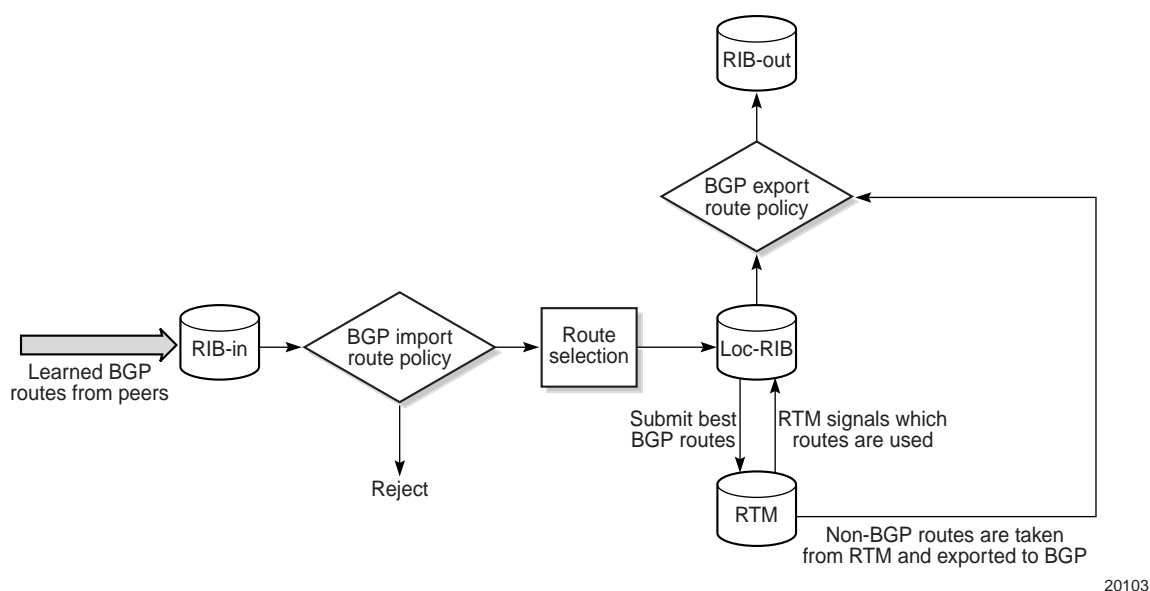
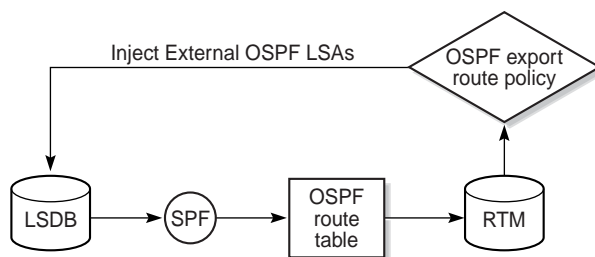


Figure 6: OSPF Route Policy Diagram



BGP Route Policies

The Alcatel-Lucent implementation of BGP uses route policies extensively. The implied or default route policies can be overridden by customized route policies. The default BGP properties, with no route policies configured, behave as follows:

- accept all BGP routes into the RTM for consideration
- announce all used BGP learned routes to other BGP peers
- announce none of the IGP, static, or local routes to BGP peers

Readvertised Route Policies

Occasionally, within the network and as applicable to the VPRN service, BGP routes may be readvertised from BGP into OSPF and IS-IS. OSPF export policies (policies control which routes are exported to OSPF) are not handled by the main OSPF task but are handled by a separate task or an RTM task that filters the routes before they are presented to the main OSPF task.

When to Use Route Policies

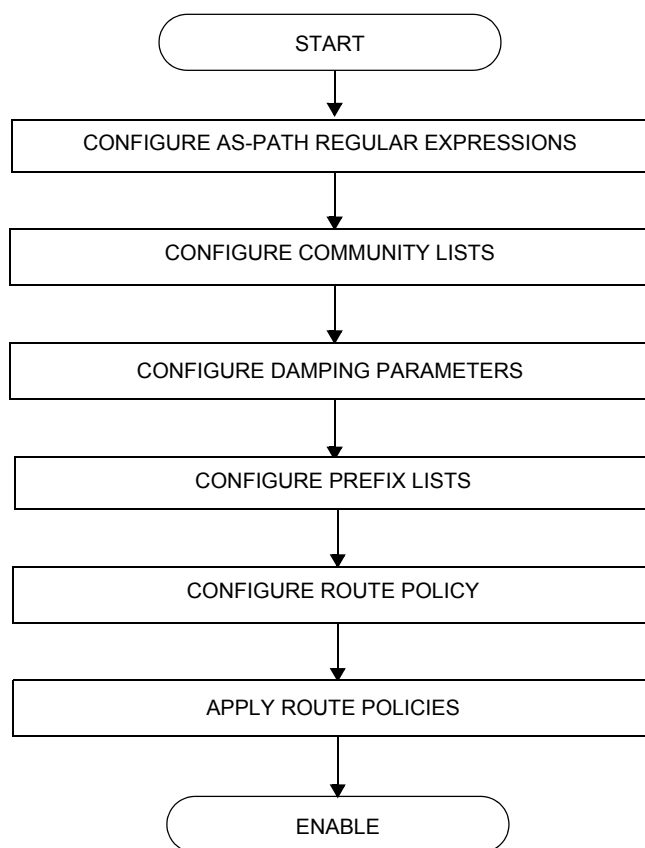
The following are examples of when to configure and apply unique route policies:

- when you want to control the protocol to allow all routes to be imported into the routing table. This enables the routing table to learn about particular routes to enable packet forwarding and redistributing of routes into other routing protocols.
 - when you want to control the export of a protocol's learned active routes
 - when you want the MP-BGP routing protocol to announce active routes learned from another routing protocol (that is, the static routes configured in the 7705 SAR). This function is sometimes called route redistribution.
 - when you want unique behaviors to control route characteristics; for example, change the route preference, AS path, or community values to manipulate or control the route selection
 - when you want to control BGP route flapping by use of route flap damping
-

Route Policy Configuration Process Overview

Figure 7 displays the process to provision basic route policy parameters.

Figure 7: Route Policy Configuration and Implementation Flow



Configuration Notes

When configuring policy statements, the policy statement name must be unique.

Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to [Standards and Protocol Support](#).

Configuring Route Policies with CLI

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

Topics in this section include:

- [Route Policy Configuration Overview on page 254](#)
 - [When to Create Routing Policies on page 254](#)
 - [Default Route Policy Actions on page 255](#)
 - [Policy Evaluation on page 256](#)
- [Basic Route Policy Configuration on page 261](#)
- [Configuring Route Policy Components on page 263](#)
 - [Beginning the Policy Statement on page 264](#)
 - [Creating a Route Policy on page 264](#)
 - [Configuring a Default Action on page 266](#)
 - [Configuring an Entry on page 267](#)
 - [Configuring an AS Path \(policy-option\) on page 269](#)
 - [Configuring a Community List on page 269](#)
 - [Configuring Damping on page 270](#)
 - [Configuring a Prefix List on page 270](#)
- [Route Policy Configuration Management Tasks on page 272](#)
 - [Editing Policy Statements and Parameters on page 272](#)
 - [Deleting an Entry on page 273](#)
 - [Deleting a Policy Statement on page 274](#)

Route Policy Configuration Overview

Route policies allow you to configure routing according to specifically defined policies. You can create policies and entries to allow or deny paths based on parameters such as source address, destination address, protocol, and community list.

Policies can be as simple or complex as required. A simple policy can block routes for a specific location or IP address. More complex policies can be configured using numerous policy statement entries containing matching conditions to specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

When to Create Routing Policies

Route policies are created in the `config>router` context. There are no default route policies. Each route policy must be explicitly created and applied. Applying route policies can introduce more efficiency as well as more complexity to the capabilities of the 7705 SAR.

Route policies are used to configure which MPLS labels should be learned or advertised. Based on the configured routing policy, MPLS labels from certain neighbors can be discarded.

Route policies are also used to control the size and content of the BGP, OSPF, and IS-IS routing tables, the routes that are advertised, and the best route to take to reach a destination.

Route policies can be created to control:

- a protocol to export all the active routes learned by that protocol
- route characteristics to control which route is selected to act as the active route to reach a destination and advertise the route to neighbors
- the protocol to import all routes into the routing table. A routing table must learn about particular routes to be able to forward packets and redistribute to other routing protocols.
- damping

Before a route policy is applied, analyze the policy's purpose and be aware of the results (and consequences) when packets match the specified criteria and the associated actions and default actions, if specified, are executed.

Default Route Policy Actions

Routing protocols have default behaviors for the import and export of routing information.

For BGP, OSPF, and IS-IS, the default route policy actions are as follows:

- BGP
 - import – all routes from BGP peers are accepted and passed to the BGP route selection process
 - export (internal routes) – all active BGP routes are advertised to BGP peers
 - export (external routes) – all non-BGP learned routes are not advertised to BGP peers (EBGP is not supported in Release 4.0 of the 7705 SAR)
- OSPF and IS-IS
 - import – not applicable; all OSPF or IS-IS routes are accepted from OSPF or IS-IS neighbors and cannot be controlled by route policies
 - export (internal routes) – all OSPF or IS-IS routes are automatically advertised to all neighbors
 - export (external routes) – all non-OSPF or non-IS-IS learned routes are not advertised to OSPF or IS-IS neighbors

Policy Evaluation

Routing policy statements can consist of one or several entries. The entries specify the matching criteria. A label is compared to the first entry in the policy statement. If it matches, the specified entry action is taken, either accepted or rejected. If the action is to accept or reject the label, that action is taken and the evaluation of the label ends.

If the label does not match the first entry, the label is compared to the next entry (if more than one is configured) in the policy statement. If there is a match with the second entry, the specified action is taken. If the action is to accept or reject the label, that action is taken and the evaluation of the label ends, and so on.

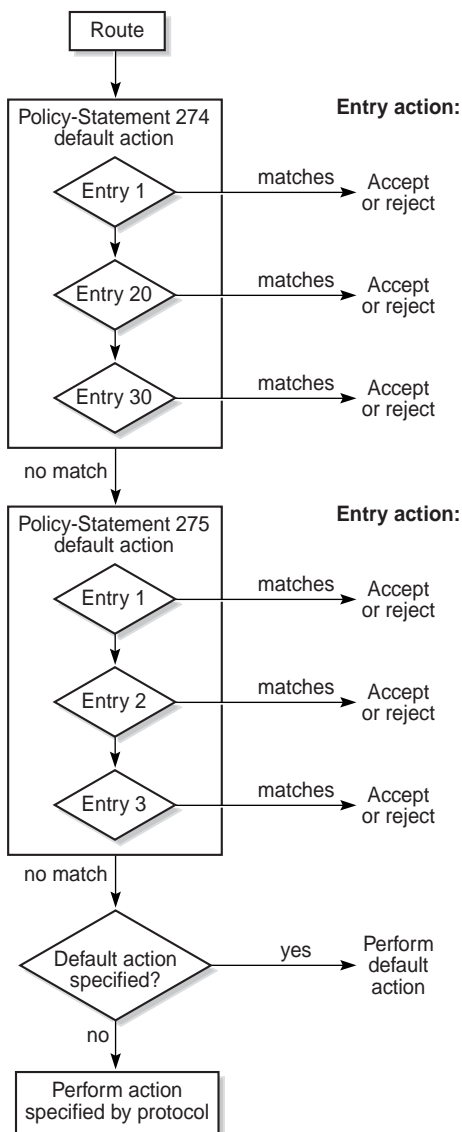
Each route policy statement can have a default-action clause defined. If a default action is defined for one or more of the configured route policies, the default action should be handled in the following ways.

- The process stops when the first complete match is found and executes the action defined in the entry.
- If the packet does not match any of the entries, the system executes the default action specified in the policy statement.

Route policies can also match a given route policy entry and continue to search for other entries within either the same route policy or the next route policy by specifying the *next-entry* or *next-policy* option in the entry's `action` command. Policies can be constructed to support multiple states to the evaluation and setting of various route attributes.

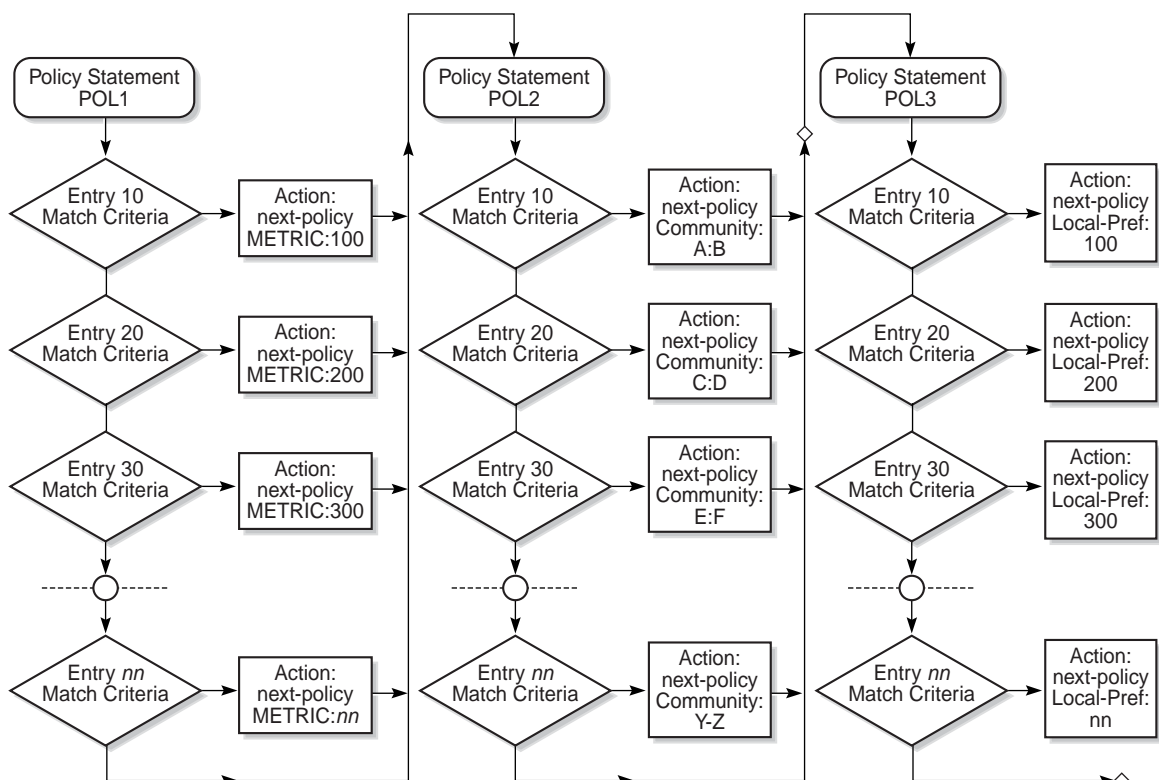
[Figure 8](#) shows an example of the route policy process.

[Figure 9](#) and [Figure 10](#) show the next-policy and next-entry route policy processes.

Figure 8: Route Policy Process Example

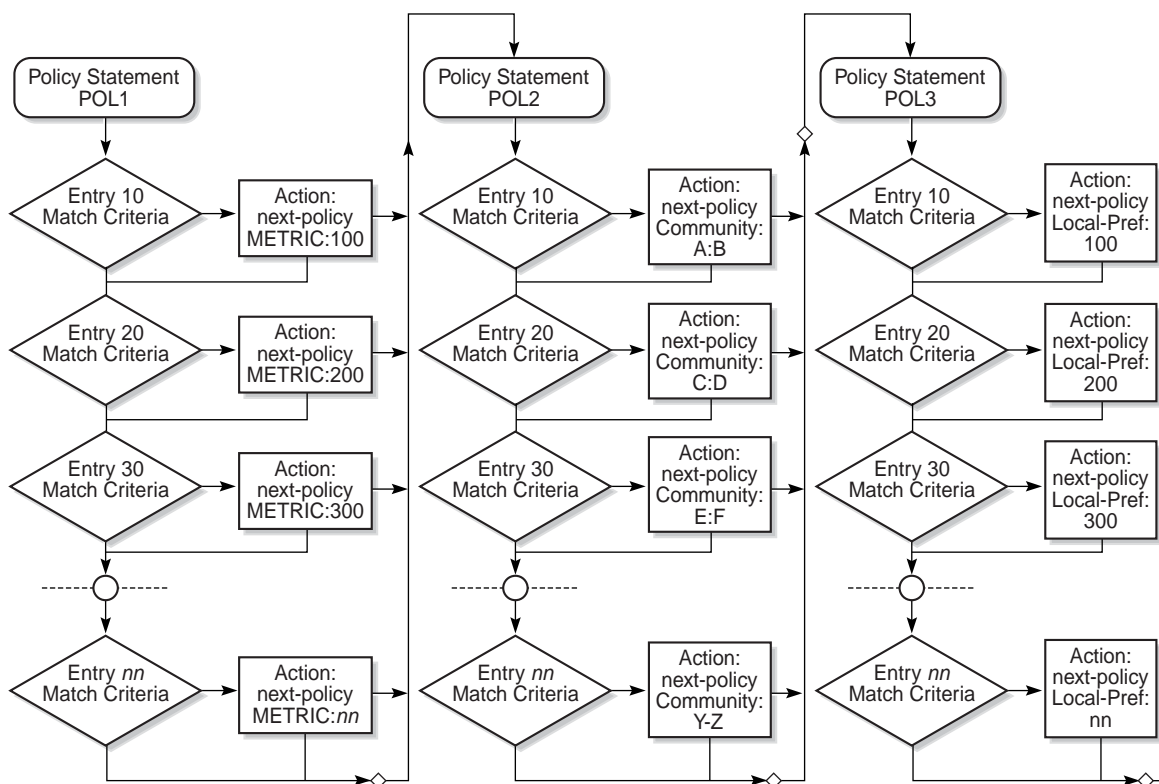
20096

Figure 9: Next Policy Logic Example



20099

Figure 10: Next Entry Logic Example



20947

Damping

Damping initiates controls when routes flap. Route flapping can occur when an advertised route between nodes alternates (flaps) back and forth between two paths due to network problems that cause intermittent route failures. To limit processing requirements, the amount of routing state change updates propagated must be reduced. Thus, when a route flaps beyond a configured value (the suppress value), then that route is removed from the routing tables and routing protocols until the value falls below the reuse value.

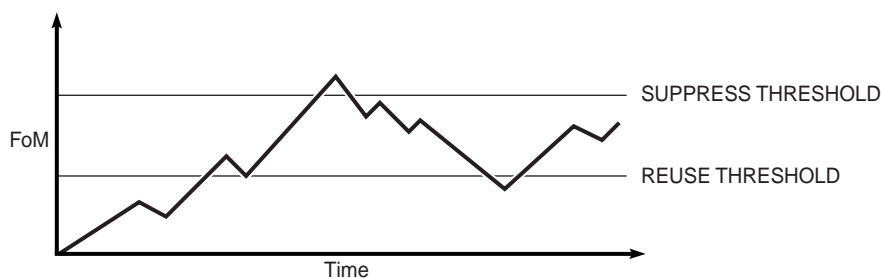
A route can be suppressed according to the Figure of Merit (FoM) value. The FoM is a value that is added to a route each time it flaps. A new route begins with an FoM value of 0.

Damping is optional. If damping is configured, the following parameter values must be explicitly specified because there are no default values:

- suppress
- half-life
- reuse
- max-suppress

When a route's FoM value exceeds the suppress value, the route is removed from the routing table. The route is considered to be stable when the FoM drops below the reuse value by means of the specified half-life parameter. The route is then returned to the routing tables. When routes have higher FoM and half-life values, they are suppressed for longer periods of time. [Figure 11](#) depicts an example of a flapping route, the suppress threshold, the half-life decay (time), and reuse threshold. The peaks represent route flaps, and the slopes represent half-life decay.

Figure 11: Damping Example



20948

Basic Route Policy Configuration

This section provides information on configuring route policies and shows configuration examples of common tasks.

The minimal route policy parameters that need to be configured are:

- policy statement with the following parameters specified:
 - at least one entry
 - entry action

The following is an example of route policy configuration, including samples for defining community members and the as-path regular expressions.

```
A:ALU-B>config>router>policy-options# info
-----
community "all-types" members "5000:[1-6][1-9][0-9]"
community "all-normal" members "5000:[1-5][1-9][0-9]"
. . .
as-path "Outside madeup paths" ".* 5001 .*"
as-path "Outside Internet paths" ".* 5002 .*"
policy-statement "RejectOutsideASPaths"
  entry 1
    from
      protocol bgp
      as-path "Outside madeup paths"
    exit
    action reject
    exit
  exit
  entry 2
    from
      protocol bgp
      as-path "Outside Internet paths"
    exit
    action reject
    exit
  exit
  entry 3
    from
      protocol ospf
    exit
    to
      protocol bgp
    exit
    action reject
    exit
  exit
```

```
entry 4
  from
    protocol isis
  exit
  to
    protocol bgp
  exit
  action reject
  exit
exit
default-action accept
exit
exit
policy-statement "aggregate-customer-peer-only"
  entry 1
    from
      community "all-customer-announce"
    exit
    action accept
    exit
  exit
  default-action reject
  exit
  exit
```

```
-----
A:ALU-B>config>router>policy-options#
```

Configuring Route Policy Components

Use the CLI syntax displayed below to configure the following:

- [Beginning the Policy Statement](#)
- [Creating a Route Policy](#)
- [Configuring a Default Action](#)
- [Configuring an Entry](#)
- [Configuring an AS Path \(policy-option\)](#)
- [Configuring a Community List](#)
- [Configuring Damping](#)
- [Configuring a Prefix List](#)

CLI Syntax:

```
config>router>policy-options
begin
commit
abort
prefix-list name
    prefix ip-prefix/mask [exact|longer|through
        length|prefix-length-range length1-length2]
policy-statement name
    description text
    default-action {accept|next-entry|next-policy|
        reject}
    entry entry-id
        description text
        action {accept|next-entry|next-policy|reject}
    from
        neighbor {ip_address|prefix-list name}
        prefix-list name [name...up to 5 max]
```

Beginning the Policy Statement

Use the following CLI syntax to begin a policy statement configuration. In order for a policy statement to be complete, an entry must be specified (see [Configuring an Entry](#)).

CLI Syntax: `config>router>policy-options`
`begin`
`policy-statement name`
`description text`

The following error message displays if you try to enter a policy options command without entering `begin` first.

```
A:ALU-B>config>router>policy-options# policy-statement "allow all"
MINOR: CLI The policy-options must be in edit mode by calling begin before any
changes can be made.
```

The following example displays policy statement configuration command usage. These commands are configured in the `config>router` context.

Example: `config>router# policy-options`
`policy-options# begin`

There are no default policy statement options. All parameters must be explicitly configured.

Creating a Route Policy

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- the `commit` command, which saves changes made to route policies during a session
- the `abort` command, which discards changes that have been made to route policies during a session

Use the following CLI syntax to enter the edit mode:

CLI Syntax: `config>router>policy-options`
`begin`

The following example displays some commands to configure a policy statement. Policy option commands are configured in the `config>router` context. Use the `commit` command to save the changes.

Example:

```
config>router>policy-options# begin
policy-options# policy-statement "allow all"
policy-options>policy-statement$ description "General
Policy"
policy-options>policy-statement>default# entry 1
policy-options>policy-statement>entry$ action accept
policy-options>policy-statement>entry# exit
policy-options>policy-statement# exit
policy-options# commit
```

The following error message displays if you try to modify a policy option without entering `begin` first.

```
A:ALU-B>config>router>policy-options# policy-statement "allow all"
MINOR: CLI The policy-options must be in edit mode by calling begin before any
changes can be made.
```

```
A:ALU-B>config>router>policy-options# info
#-----
# Policy
#-----

    policy-options
        begin
        policy-statement "allow all"
        description "General Policy"
        ...
        exit
    exit
-----
A:ALU-B>config>router>policy-options#
```

Configuring a Default Action

Specifying a default action is optional. The default action controls those packets not matching any policy statement entries. The default action is applied only to those routes that do not match any policy entries.

If no default action is specified and there is no match, the packets will be accepted.

A policy statement must include at least one entry (see [Configuring an Entry](#)).

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- the `commit` command, which saves changes made to route policies during a session
- the `abort` command, which discards changes made to route policies during a session

CLI Syntax:

```
config>router>policy-options
begin
commit
abort
policy-statement name
    default-action {accept | next-entry | next-policy |
    reject}
        as-path {add | replace} name
        community {add | remove | replace} name
        damping name
        metric {add | subtract | set} metric
        preference preference
        tag hex-string
        type type
```

The following example displays default action configuration command usage. These commands are configured in the `config>router>policy-options` context.

Example:

```
config>router>policy-options# policy-statement "1"
policy-statement$ default-action accept
```

The following example displays the default action configuration:

```
A:ALU-B>config>router>policy-options# info
-----
    policy-statement "1"
      default-action accept
      as-path add "saratoga"
      community add "365"
      damping "flaptest"
      next-hop 10.10.10.104
    exit
      type 1
    exit
-----
A:ALU-B>config>router>policy-options#
```

Configuring an Entry

An entry action must be specified. The other parameters in the `entry>action` context are optional.

CLI Syntax:

```
config>router>policy-options
begin
commit
abort
policy-statement name
  entry entry-id
    description text
    action {accept | next-entry | next-policy | reject}
    from
      area area-id
      as-path {add | replace} name
      community name members comm-id
      external
      family [ipv4] [vpn-ipv4]
      interface interface-name
      level {1 | 2}
      neighbor {ip-address | prefix-list name}
      origin {igp | egp | incomplete | any}
      prefix-list name [name...(up to 5 max)]
      protocol protocol
      tag tag
      type type
    to
      level {1 | 2}
      neighbor {ip-address | prefix-list name}
      prefix-list name [name...(up to 5 max)]
      protocol protocol
```

The following example displays entry command usage. These commands are configured in the `config>router>policy-options` context.

Example:

```
config>router>policy-options# policy-statement "1"
policy-statement# entry 1
policy-statement>entry$ to
policy-statement>entry>to# protocol bgp
policy-statement>entry>to# neighbor 10.10.10.104
policy-statement>entry>to# exit
policy-statement>entry# action accept
policy-statement>entry>action# exit
policy-statement>entry# exit
policy-statement# entry 2
policy-statement>entry$ from
policy-statement>entry>from# protocol ospf
policy-statement>entry>from# exit
policy-statement>entry$ to
policy-statement>entry>to# protocol ospf
policy-statement>entry>to# neighbor 10.10.0.91
policy-statement>entry>to# exit
policy-statement>entry# action accept
policy-statement>entry>action# exit
```

The following example displays entry parameters and includes the default action parameters that were displayed in the previous section.

```
A:ALU-B>config>router>policy-options# info
-----
policy-statement "1"
  entry 1
    to
      protocol bgp
      neighbor 10.10.10.104
    exit
    action accept
    exit
  exit
  entry 2
    from
      protocol ospf
    exit
    to
      protocol ospf
      neighbor 10.10.0.91
    exit
    action accept
    exit
  exit
  default-action accept
  . . .
  exit
exit
-----
```

Configuring an AS Path (policy-option)

An AS path is defined by a regular expression in the `config>router>policy-options` context. Once defined, it can be added, removed, or replaced in a policy statement as part of a default action, an entry action, or an entry from (source) definition. See [Configuring a Default Action](#) and [Configuring an Entry](#).

The following example displays `as-path` command usage.

```
A:ALU-B>config>router># info
-----
. . .
  as-path "Outside madeup paths" ".* 5001 .*"
  as-path "Outside Internet paths" ".* 5002 .*"
. . .
-----
A:ALU-B>config>router>#
```

Configuring a Community List

Community lists are composed of a group of destinations that share a common property. Community lists allow you to administer actions on a configured group instead of having to execute identical commands for each member.

The following example displays a community list configuration:

```
A:ALU-B>config>router>policy-options# info
-----
community "eastern" members "100:200"
community "western" members "100:300"
community "northern" members "100:400"
community "southern" members "100:500"
community "headquarters" members "100:1000"
policy-statement "1"
  entry 1
    to
      protocol bgp
      neighbor 10.10.10.104
    exit
    action accept
. . .
-----
A:ALU-B>config>router>policy-options#
```

Configuring Damping

Observe the following items when configuring damping.

- For each damping profile, all parameters must be configured.
- The suppress value must be greater than the reuse value (see [Figure 11](#)).
- Damping can be enabled in the `config>router>bgp` context on the BGP global, group, and neighbor levels. If damping is enabled but route policy does not specify a damping profile, the default damping profile will be used. This profile is always present and consists of the following parameters:
 - half-life: 15 min
 - max-suppress: 60 min
 - suppress: 3000
 - reuse: 750

The following example displays a damping configuration:

```
A:ALU-B>config>router>policy-options# info
-----
      damping "dampstest123"
        half-life 15
        max-suppress 60
        reuse 750
        suppress 1000
      exit
-----
A:ALU-B>config>router>policy-options#
```

Configuring a Prefix List

Use the following CLI syntax to configure a prefix list:

CLI Syntax: `prefix-list name`
`prefix ip-prefix/mask [exact|longer|through`
`length/prefix-length-range length1-length2]`

The following example displays prefix list configuration command usage. These commands are configured in the `config>router` context.

Example:

```
config>router>policy-options# prefix-list
policy-options# prefix-list western
policy-options>prefix-list# prefix 10.10.0.1/32
policy-options>prefix-list# prefix 10.10.0.2/32
policy-options>prefix-list# prefix 10.10.0.3/32
policy-options>prefix-list# prefix 10.10.0.4/32
```

The following example displays the prefix list configuration.

```
A:ALU-B>config>router>policy-options# info
-----
      prefix-list "western"
        prefix 10.10.0.1/32 exact
        prefix 10.10.0.2/32 exact
        prefix 10.10.0.3/32 exact
        prefix 10.10.0.4/32 exact
      exit
-----
A:ALU-B>config>router>policy-options>#
```

Route Policy Configuration Management Tasks

This section discusses the following route policy configuration management tasks:

- [Editing Policy Statements and Parameters](#)
- [Deleting an Entry](#)
- [Deleting a Policy Statement](#)

Editing Policy Statements and Parameters

Route policy statements can be edited to modify, add, or delete parameters. To enter edit mode, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- the `commit` command, which saves changes made to route policies during a session
- the `abort` command, which discards changes that have been made to route policies during a session

The following example displays some commands to configure a policy statement. These commands are configured in the `config>router>policy-options` context.

Example:

```
config>router>policy-options# begin
policy-options# policy-statement "1"
policy-statement# description "Level 1"
policy-statement# entry 4
policy-statement>entry$ description "new entry"
policy-statement>entry# from
policy-statement>entry>from$ prefix-list "from hq"
policy-statement>entry>from# exit
policy-statement>entry# action reject
policy-statement>entry# commit
policy-statement>entry# exit
```


The following example displays the changed configuration.

```
A:ALU-B>config>router>policy-options>policy-statement# info
-----
description "Level 1"
entry 1
  from
    neighbor 10.10.10.104
  exit
  action accept
  exit
exit
entry 2
  from
    prefix-list list1
  exit
  from
    neighbor 10.10.0.91
  exit
  action accept
  exit
exit
entry 4
  description "new entry"
  from
    prefix-list "from hq"
  exit
  action reject
exit
default-action accept
exit
-----
A:ALU-B>config>router>policy-options>policy-statement#
```

Deleting an Entry

Use the following CLI syntax to delete a policy statement entry:

CLI Syntax: config>router>policy-options
 begin
 commit
 abort
 policy-statement *name*
 no entry *entry-id*

The following example displays the commands required to delete a policy statement entry.

Example: config>router>policy-options# begin
 policy-options# policy-statement "1"
 policy-options>policy-statement# no entry 4
 policy-options>policy-statement# commit

Deleting a Policy Statement

Use the following CLI syntax to delete a policy statement:

CLI Syntax: `config>router>policy-options`
`begin`
`commit`
`abort`
`no policy-statement name`

The following example displays the commands required to delete a policy statement.

Example: `config>router>policy-options# begin`
`policy-options# no policy-statement 1`
`policy-options# commit`

Route Policy Command Reference

Command Hierarchies

- [Route Policy Configuration Commands](#)
- [Show Commands](#)

Route Policy Configuration Commands

```

config
  — [no] router
    — [no] policy-options
      — abort
      — as-path name {regular-expression | null}
      — no as-path name
      — begin
      — commit
      — community name members comm-id [comm-id ... (up to 15 max)]
      — no community name members comm-id
      — [no] damping name
        — half-life minutes
        — no half-life
        — max-suppress minutes
        — no max-suppress
        — reuse integer
        — no reuse
        — suppress integer
        — no suppress
      — [no] policy-statement name
        — description description-string
        — no description
        — default-action {accept | next-entry | next-policy | reject}
        — no default-action
          — as-path {add | replace} name
          — no as-path
          — as-path-prepend as-number [repeat]
          — no as-path-prepend
          — community {{add name [remove name]} | {remove name
            [add name]} | {replace name}}
          — no community
          — damping {name | none}
          — no damping
          — local-preference preference
          — no local-preference
          — metric {add | subtract | set} metric

```

```

— no metric
— next-hop ip-address
— no next-hop
— [no] next-hop-self
— origin {igp | egp | incomplete}
— no origin
— metric {add | subtract | set} metric
— no metric
— preference preference
— no preference
— tag hex-string
— no tag
— type type
— no type
— entry entry-id
— no entry
  — description description-string
  — no description
  — action {accept | next-entry | next-policy | reject}
  — no action
    — as-path {add | replace} name
    — no as-path
    — as-path-prepend as-number [repeat]
    — no as-path-prepend
    — community { {add name [remove name] } |
      {remove name [add name] } | {replace name} }
    — no community
    — damping {name | none}
    — no damping
    — local-preference preference
    — no local-preference
    — metric {add | subtract | set} metric
    — no metric
    — next-hop ip-address
    — no next-hop
    — [no] next-hop-self
    — origin {igp | egp | incomplete}
    — no origin
    — preference preference
    — no preference
    — tag hex-string
    — no tag
    — type type
    — no type
  — [no] from
    — area area-id
    — no area
    — as-path name
    — no as-path
    — community name
    — no community
    — [no] external
    — family [ipv4] [vpn-ipv4]
    — no family

```

```

— interface interface-name
— no interface
— level {1 | 2}
— no level
— neighbor {ip-address | prefix-list name}
— no neighbor
— origin {igp | egp | incomplete | any}
— no origin
— prefix-list name [name...(up to 5 max)]
— no prefix-list
— protocol protocol
— no protocol
— tag tag
— no tag
— type type
— no type
— [no] to
— level {1 | 2}
— no level
— neighbor {ip-address | prefix-list name}
— no neighbor
— prefix-list name [name...(up to 5 max)]
— no prefix-list
— protocol protocol
— no protocol
— [no] prefix-list name
— [no] prefix ip-prefix/prefix-length [exact | longer | through length |
prefix-length-range length1-length2]
— [no] triggered-policy

```

Show Commands

```

show
— router router-name
— policy [name | damping | prefix-list name | as-path name | community name | admin]

```

Command Descriptions

- [Configuration Commands on page 279](#)
- [Show Commands on page 303](#)

Configuration Commands

- [Generic Commands on page 280](#)
- [Route Policy Options on page 282](#)
- [Route Policy Damping Commands on page 285](#)
- [Route Policy Prefix Commands on page 288](#)
- [Route Policy Entry Match Commands on page 289](#)
- [Route Policy Action Commands on page 296](#)

Generic Commands

abort

Syntax	abort
Context	config>router>policy-options
Description	This command discards changes made to a route policy.
Default	n/a

begin

Syntax	begin
Context	config>router>policy-options
Description	This command enters the mode to create or edit route policies.
Default	n/a

commit

Syntax	commit
Context	config>router>policy-options
Description	This command saves changes made to a route policy.
Default	n/a

description

Syntax	description <i>description-string</i> no description
Context	config>router>policy-options>policy-statement config>router>policy-options>policy-statement>entry
Description	<p>This command creates a text description that is stored in the configuration file to help identify the contents of the entity.</p> <p>The no form of the command removes the string from the configuration.</p>
Default	n/a
Parameters	<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, etc.), the entire string must be enclosed within double quotes.

Route Policy Options

as-path

Syntax	as-path <i>name</i> { <i>regular-expression</i> null } no as-path <i>name</i>
Context	config>router>policy-options
Description	This command creates a route policy AS path regular expression statement to use in route policy entries. The no form of the command deletes the AS path regular expression statement.
Default	no as-path
Parameters	<i>name</i> — the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. <i>regular-expression</i> — the AS path regular expression. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. null — the AS path expressed as an empty regular expression string

community

Syntax	community <i>name</i> members <i>comm-id</i> [<i>comm-id</i> ...(up to 15 max)] no community <i>name</i> [members <i>comm-id</i>]
Context	config>router>policy-options
Description	This command creates a route policy community list to use in route policy entries. The no form of the command deletes the community list or the provided community ID.
Default	no community
Parameters	<i>name</i> — the community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

comm-id — the community ID. Up to 15 community ID strings can be specified with a total maximum of 72 characters. A community ID can be specified in four different forms:

as-number:comm-val1 | *reg-ex* | *ext-comm* | *well-known-comm*

Values *as-number:comm-val1* — the *as-number* is the Autonomous System Number (ASN), where:

as-number: 0 to 65535

comm-val1: 0 to 65535

reg-exp — a regular expression string. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

ext-comm — where *ext-comm* is defined as *type:{ip-address:comm-val1 | as-number:comm-val2}* and where:

type: **target** or **origin** (keywords that denote the community as an extended community of type route target or route origin, respectively)

ip-address: a.b.c.d

comm-val1: 0 to 65535

as-number: 0 to 65535

comm-val2: 0 to 4294967295 (*as-number* and *comm.-val2* allow the same values as described above for regular community values)

well-known-comm — one of the keywords **no-advertise**, **no-export**, **no-export-subconfed**, **none**

policy-options

Syntax	[no] policy-options
Context	config>router
Description	<p>This command enables the context to configure route policies. Route policies are applied to the routing protocol.</p> <p>The no form of the command deletes the route policy configuration.</p>
Default	n/a

policy-statement

Syntax	[no] policy-statement <i>name</i>
Context	config>router>policy-options
Description	<p>This command creates the context to configure a route policy statement.</p> <p>Route policy statements control the flow of routing information from a specific protocol or protocols.</p> <p>The policy-statement is a logical grouping of match and action criteria. A single policy-statement can affect routing in one or more protocols and/or one or more protocols' peers/neighbors. A single policy-statement can also affect the export of routing information.</p> <p>The no form of the command deletes the policy statement.</p>
Default	no policy-statement
Parameters	<i>name</i> — the route policy statement name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

triggered-policy

Syntax	[no] triggered-policy
Context	config>router
Description	<p>This command triggers route policy re-evaluation.</p> <p>By default, when a change is made to a policy in the config router policy-options context and then committed, the change is effective immediately. However, there may be circumstances where the changes should or must be delayed; for example, when a policy change is implemented that would affect every BGP peer on a 7705 SAR. It is more effective to control changes on a peer-by-peer basis.</p> <p>If the triggered-policy command is enabled and a given peer is established, and you want the peer to remain up, then, in order for a change to a route policy to take effect, a clear command with the soft or soft-inbound option must be used. In other words, when a triggered-policy is enabled, any routine policy change or policy assignment change within the protocol will not take effect until the protocol is reset or a clear command is issued to re-evaluate route policies; for example, clear router bgp neighbor x.x.x.x soft. This keeps the peer up, and the change made to a route policy is applied only to that peer, or group of peers.</p>
Default	disabled — dynamic route policy is enabled; policy-option configuration changes take effect immediately

Route Policy Damping Commands

damping

Syntax	[no] damping <i>name</i>
Context	config>router>policy-options
Description	This command creates a context to configure a route damping profile to use in route policy entries. The no form of the command deletes the named route damping profile.
Default	no damping
Parameters	<i>name</i> — the damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

half-life

Syntax	half-life <i>minutes</i> no half-life
Context	config>router>policy-options>damping
Description	This command configures the half-life parameter for the route damping profile. The half-life value is the time, expressed in minutes, required for a route to remain stable in order for the Figure of Merit (FoM) value to be reduced by one half; for example, if the half-life value is 6 and the route remains stable for 6 min, then the new FoM value is 3. After another 3 min pass and the route remains stable, the new FoM value is 1.5 (minutes). When the FoM value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements. The no form of the command removes the half-life parameter from the damping profile.
Default	no half-life
Parameters	<i>minutes</i> — the half-life in minutes expressed as a decimal integer Values 1 to 45

max-suppress

Syntax	max-suppress <i>minutes</i> no max-suppress
Context	config>router>policy-options>damping
Description	<p>This command configures the maximum suppression parameter for the route damping profile.</p> <p>This value indicates the maximum time, expressed in minutes, that a route can remain suppressed.</p> <p>The no form of the command removes the maximum suppression parameter from the damping profile.</p>
Default	no max-suppress
Parameters	<i>minutes</i> — the maximum suppression time, in minutes, expressed as a decimal integer
Values	1 to 720

reuse

Syntax	reuse <i>integer</i> no reuse
Context	config>router>policy-options>damping
Description	<p>This command configures the reuse parameter for the route damping profile.</p> <p>When the Figure of Merit (FoM) value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements.</p> <p>The no form of the command removes the reuse parameter from the damping profile.</p>
Default	no reuse
Parameters	<i>integer</i> — the reuse value expressed as a decimal integer
Values	1 to 20000

suppress

Syntax	suppress <i>integer</i> no suppress
Context	config>router>policy-options>damping
Description	<p>This command configures the suppression parameter for the route policy damping profile.</p> <p>A route is suppressed when it has flapped frequently enough to increase the Figure of Merit (FoM) value so that it exceeds the suppress threshold limit. When the FoM value exceeds the suppress threshold limit, the route is removed from the route table or inclusion in advertisements.</p> <p>The no form of the command removes the suppress parameter from the damping profile.</p>
Default	no suppress
Parameters	<i>integer</i> — the suppress value expressed as a decimal integer
Values	1 to 20000

Route Policy Prefix Commands

prefix-list

Syntax	[no] prefix-list <i>name</i>
Context	config>router>policy-options
Description	This command creates a context to configure a prefix list to use in route policy entries. The no form of the command deletes the named prefix list.
Default	n/a
Parameters	<i>name</i> — the prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

prefix

Syntax	[no] prefix <i>ip-prefix/prefix-length</i> [exact longer through <i>length</i> prefix-length-range <i>length1-length2</i>]										
Context	config>router>policy-options>prefix-list										
Description	<p>This command creates a prefix entry in the route policy prefix list.</p> <p>The no form of the command deletes the prefix entry from the prefix list.</p>										
Parameters	<p><i>ip-prefix/prefix-length</i> — the IP prefix for the prefix list entry in dotted-decimal notation</p> <table><tr><td>Values</td><td>ipv4:</td><td>a.b.c.d (host bits must be 0)</td></tr><tr><td></td><td>ipv4-prefix-length:</td><td>0 to 32</td></tr></table> <p>exact — the prefix list entry only matches the route with the specified <i>ip-prefix</i> and <i>prefix-length</i> values</p> <p>longer — the prefix list entry matches any route that matches the specified <i>ip-prefix</i> and has a <i>prefix-length</i> value greater than the specified <i>prefix-length</i></p> <p><i>length</i> — the prefix list entry matches any route that matches the specified <i>ip-prefix</i> and has a <i>prefix-length</i> value within the specified <i>length</i> values</p> <table><tr><td>Values</td><td>0 to 32</td></tr></table> <p><i>length1 - length2</i> — a route must match the most significant bits and have a <i>prefix-length</i> value within the given range</p> <table><tr><td>Values</td><td>0 to 32, <i>length2</i> > <i>length1</i> > <i>prefix-length</i></td></tr></table>	Values	ipv4:	a.b.c.d (host bits must be 0)		ipv4-prefix-length:	0 to 32	Values	0 to 32	Values	0 to 32, <i>length2</i> > <i>length1</i> > <i>prefix-length</i>
Values	ipv4:	a.b.c.d (host bits must be 0)									
	ipv4-prefix-length:	0 to 32									
Values	0 to 32										
Values	0 to 32, <i>length2</i> > <i>length1</i> > <i>prefix-length</i>										

Route Policy Entry Match Commands

entry

Syntax	entry <i>entry-id</i> no entry
Context	config>router>policy-options>policy-statement
Description	<p>This command creates the context to edit route policy entries within the route policy statement.</p> <p>Multiple entries can be created using unique entries. The 7705 SAR OS exits the filter when the first match is found and executes the action specified. For this reason, entries must be sequenced correctly from most to least explicit.</p> <p>An entry does not require matching criteria defined (in which case, everything matches) but must have an action defined in order to be considered complete. Entries without an action are considered incomplete and will be rendered inactive.</p> <p>The no form of the command removes the specified entry from the route policy statement.</p>
Default	n/a
Parameters	<p><i>entry-id</i> — the entry ID expressed as a decimal integer. An <i>entry-id</i> uniquely identifies match criteria and the corresponding action. It is recommended that multiple entries be given <i>entry-ids</i> in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.</p> <p>Values 1 to 4294967295</p>

from

Syntax	[no] from
Context	config>router>policy-options>policy-statement>entry
Description	<p>This command creates the context to configure policy match criteria based on a route's source or the protocol from which the route is received.</p> <p>If no condition is specified, all route sources are considered to match.</p> <p>The no form of the command deletes the source match criteria for the route policy statement entry.</p>

to

Syntax	[no] to
Context	config>router>policy-options>policy-statement>entry
Description	<p>This command creates the context to configure export policy match criteria based on a route's destination or the protocol into which the route is being advertised.</p> <p>If no condition is specified, all route destinations are considered to match.</p> <p>The to command context only applies to export policies. If it is used for an import policy, match criteria is ignored.</p> <p>The no form of the command deletes export match criteria for the route policy statement entry.</p>

area

Syntax	area <i>area-id</i> no area
Context	config>router>policy-options>policy-statement>entry>from
Description	<p>This command configures an OSPF area as a route policy match criterion.</p> <p>This match criterion is only used in export policies.</p> <p>All OSPF routes (internal and external) are matched using this criterion if the best path for the route is by the specified area.</p> <p>The no form of the command removes the OSPF area match criterion.</p>
Default	n/a
Parameters	<i>area-id</i> — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer
Values	0.0.0.0 to 255.255.255.255 (dotted-decimal), 0 to 4294967295 (decimal)

as-path

Syntax	as-path <i>name</i> no as-path
Context	config>router>policy-options>policy-statement>entry>from
Description	<p>This command configures an AS path regular expression statement as a match criterion for the route policy entry. If no AS path criterion is specified, any AS path is considered to match. AS path regular expression statements are configured at the global route policy level (config>router>policy-options>as-path <i>name</i>).</p>

The **no** form of the command removes the AS path regular expression statement as a match criterion.

Default **no as-path**

Parameters *name* — the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

The *name* specified must already be defined.

community

Syntax **community** *name*
no community

Context config>router>policy-options>policy-statement>entry>from

Description This command configures a community list as a match criterion for the route policy entry. If no community list is specified, any community is considered a match.

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

Default **no community**

Parameters *name* — the community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

The *name* specified must already be defined.

external

Syntax [**no**] **external**

Context config>router>policy-options>policy-statement>entry>from

Description This command specifies the external IS-IS route matching criteria for the entry.

Default **no external**

family

Syntax **family** [ipv4] [vpn-ipv4]
no family

Context config>router>policy-options>policy-statement>entry>from

Description This command specifies address families as matching conditions.

- Parameters** **ipv4** — specifies IPv4 routing information
- vpn-ipv4** — specifies VPN-IPv4 routing information

interface

- Syntax** **interface** *interface-name*
 no interface
- Context** config>router>policy-options>policy-statement>entry>from
- Description** This command specifies the router interface, specified either by name or address, as a filter criterion.
- The **no** form of the command removes the criterion from the configuration.
- Default** **no interface**
- Parameters** *interface-name* — the name of the interface used as a match criterion for this entry. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

level

- Syntax** **level** {1 | 2}
 no level
- Context** config>router>policy-options>policy-statement>entry>from
 config>router>policy-options>policy-statement>entry>to
- Description** This command specifies the IS-IS route level as a match criterion for the entry.
- Default** **no level**
- Parameters** 1 | 2 — matches the IS-IS route learned from level 1 or level 2

neighbor

- Syntax** **neighbor** {*ip-address* | **prefix-list** *name*}
 no neighbor
- Context** config>router>policy-options>policy-statement>entry>from
 config>router>policy-options>policy-statement>entry>to
- Description** This command specifies the neighbor address as found in the source address of the actual join and prune message as a filter criterion. If no neighbor is specified, any neighbor is considered a match.
- The **no** form of the command removes the neighbor IP match criterion from the configuration.

Default	no neighbor
Parameters	<i>ip-address</i> — the neighbor IP address in dotted-decimal notation
	Values a.b.c.d
	<i>name</i> — the prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.
	The <i>name</i> specified must already be defined.

origin

Syntax	origin {igp egp incomplete any} no origin
Context	config>router>policy-options>policy-statement>entry>from
Description	This command configures a BGP origin attribute as a match criterion for a route policy statement entry. If no origin attribute is specified, any BGP origin attribute is considered a match. The no form of the command removes the BGP origin attribute match criterion.
Default	no origin
Parameters	igp — configures matching path information originating within the local AS egp — configures matching path information originating in another AS incomplete — configures matching path information learned by another method any — ignores this criteria

prefix-list

Syntax	prefix-list name [name...(up to 5 max)] no prefix-list
Context	config>router>policy-options>policy-statement>entry>from config>router>policy-options>policy-statement>entry>to
Description	This command configures a prefix list as a match criterion for a route policy statement entry. If no prefix list is specified, any network prefix is considered a match. The prefix list specifies the network prefix (this includes the prefix and length) that a specific policy entry applies to. Up to five prefix list names can be specified.

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

Default **no prefix-list**

Parameters *name* — the prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

protocol

Syntax **protocol** *protocol*
no protocol

Context config>router>policy-options>policy-statement>entry>from
config>router>policy-options>policy-statement>entry>to

Description This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending how it is used.

If no protocol criterion is specified, any protocol is considered a match.

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

Default **no protocol**

Parameters *protocol* — the protocol name to match

Values bgp, direct, ospf, isis, static, aggregate, bgp-vpn, ldp

tag

Syntax **tag** *tag*
no tag

Context config>router>policy-options>policy-statement>entry>from

Description This command adds an integer tag to the static route. These tags are then matched to control route redistribution.

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

Default **no tag**

Parameters *tag* — matches a specific external LSA tag field

Values 1 to 4294967295

type

Syntax	type <i>type</i> no type
Context	config>router>policy-options>policy-statement>entry>from
Description	<p>This command configures an OSPF type metric as a match criterion in the route policy statement entry.</p> <p>If no type is specified, any OSPF type is considered a match.</p> <p>The no form of the command removes the OSPF type match criterion.</p>
Parameters	<i>type</i> — the OSPF type metric
Values	1 — set as OSPF routes with type 1 LSAs 2 — set as OSPF routes with type 2 LSAs

Route Policy Action Commands

default-action

Syntax	default-action {accept next-entry next-policy reject} no default-action
Context	config>router>policy-options>policy-statement
Description	<p>This command enables the context to configure actions for routes that do not match any route policy statement entries when the accept parameter is specified.</p> <p>The default action clause can be set to all available action states including: accept, reject, next-entry, and next-policy. If the action states accept or reject, the policy evaluation terminates and the appropriate result is returned.</p> <p>If a default action is defined and no match(es) occurred with the entries in the policy, the default action clause is used.</p> <p>If a default action is defined and one or more matches occurred with the entries of the policy, the default action is not used.</p> <p>The no form of the command deletes the default-action context for the policy statement.</p>
Default	no default-action
Parameters	<p>accept — routes matching the entry match criteria will be accepted and propagated</p> <p>next-entry — the actions specified will be made to the route attributes and then policy evaluation will continue with the next policy entry (if any others are specified)</p> <p>next-policy — the actions specified will be made to the route attributes and then policy evaluation will continue with the next route policy (if any others are specified)</p> <p>reject — routes matching the entry match criteria will be rejected</p>

action

Syntax	action {accept next-entry next-policy reject} no action
Context	config>router>policy-options>policy-statement>entry
Description	<p>This command creates the context to configure actions to take for routes matching a route policy statement entry.</p> <p>This command is required and must be entered for the entry to be active.</p>

Any route policy entry without the **action** command will be considered incomplete and will be inactive.

The **no** form of the command deletes the action context from the entry.

Default **no action**

Parameters **accept** — specifies that routes matching the entry match criteria will be accepted and propagated

next-entry — the actions specified will be made to the route attributes and then policy evaluation will continue with the next policy entry (if any others are specified)

next-policy — the actions specified will be made to the route attributes and then policy evaluation will continue with the next route policy (if any others are specified)

reject — routes matching the entry match criteria will be rejected

as-path

Syntax **as-path {add | replace} name**
no as-path

Context config>router>policy-options>policy-statement>default-action
 config>router>policy-options>policy-statement>entry>action

Description This command assigns a BGP AS path list to routes matching the route policy statement entry. If no AS path list is specified, the AS path attribute is not changed.

The **no** form of the command disables the AS path list editing action from the route policy entry.

Default **no as-path**

Parameters **add** — the AS path list is to be prepended to an existing AS list

replace — the AS path list replaces any existing AS path attribute

name — the AS path list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. The name specified must already be defined.

as-path-prepend

Syntax	as-path-prepend <i>as-num</i> [<i>repeat</i>] no as-path-prepend
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	<p>This command prepends a BGP AS number once or numerous times to the AS path attribute of routes matching the route policy statement entry. If an AS number is not configured, the AS path is not changed.</p> <p>If the optional number is specified, then the AS number is prepended as many times as indicated by the number.</p> <p>The no form of the command disables the AS path prepend action from the route policy entry.</p>
Default	no as-path-prepend
Parameters	<i>as-num</i> — the AS number to prepend expressed as a decimal integer Values 1 to 4294967295 <i>repeat</i> — the number of times to prepend the specified AS number expressed as a decimal integer Values 1 to 50

community

Syntax	community {{ add <i>name</i> [remove <i>name</i>]} { remove <i>name</i> [add <i>name</i>]} { replace <i>name</i> }} no community
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	<p>This command adds or removes a BGP community list to or from routes matching the route policy statement entry. If no community list is specified, the community path attribute is not changed.</p> <p>The community list changes the community path attribute according to the add and remove keywords.</p> <p>The no form of the command disables the action to edit the community path attribute for the route policy entry.</p>
Default	no community

Parameters	add — the specified community list is added to any existing list of communities
	remove — the specified community list is removed from the existing list of communities
	replace — the specified community list replaces any existing community attribute
	<i>name</i> — the community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

damping

Syntax	damping { <i>name</i> none } no damping
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	This command configures a damping profile used for routes matching the route policy statement entry. If no damping criteria is specified, the default damping profile is used. The no form of the command removes the damping profile associated with the route policy entry.
Default	no damping
Parameters	<i>name</i> — the damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. The name specified must already be defined. none — disables route damping for the route policy

local-preference

Syntax	local-preference <i>preference</i> no local-preference
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry
Description	This command assigns a BGP local preference to routes matching a route policy statement entry. If no local preference is specified, the BGP configured local preference is used. The no form of the command disables assigning a local preference in the route policy entry.
Default	no local-preference
Parameters	<i>preference</i> — the local preference expressed as a decimal integer Values 0 to 4294967295

metric

Syntax	metric { add subtract set } <i>metric</i> no metric
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	<p>This command assigns a metric to routes that do not match any entry (for default action) or that match the entry (for action).</p> <p>If no metric is specified, the configured metric is used. If neither is defined, no metric will be advertised.</p> <p>The value assigned for the metric by the route policy is controlled by the required keywords.</p> <p>The no form of the command disables assigning a metric in the route policy entry.</p>
Default	no metric
Parameters	<p>add — the specified metric is added to any existing metric. If the result of the addition results in a number greater than 4294967295, the value 4294967295 is used.</p> <p>subtract — the specified metric is subtracted from any existing metric. If the result of the subtraction results in a number less than 0, the value of 0 is used.</p> <p>set — the specified metric replaces any existing metric</p> <p><i>metric</i> — the metric modifier expressed as a decimal integer</p> <p>Values 0 to 4294967295</p>

next-hop

Syntax	next-hop <i>ip-address</i> no next-hop				
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action				
Description	<p>This command assigns the specified next-hop IP address to routes matching the policy statement entry. If a next-hop IP address is not specified, the next-hop attribute is not changed.</p> <p>The no form of the command disables assigning a next-hop address in the route policy entry.</p>				
Default	no next-hop				
Parameters	<i>ip-address</i> — the next-hop IP address in dotted-decimal notation				
Values	<table><tr><td><i>ipv4-prefix:</i></td><td>a.b.c.d (host bits must be 0)</td></tr><tr><td><i>ipv4-prefix-length:</i></td><td>0 to 32</td></tr></table>	<i>ipv4-prefix:</i>	a.b.c.d (host bits must be 0)	<i>ipv4-prefix-length:</i>	0 to 32
<i>ipv4-prefix:</i>	a.b.c.d (host bits must be 0)				
<i>ipv4-prefix-length:</i>	0 to 32				

next-hop-self

Syntax	[no] next-hop-self
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	This command advertises a next-hop IP address belonging to this router even if a third-party next hop is available to routes matching the policy statement entry. The no form of the command disables advertising the next-hop-self option for the route policy entry.
Default	no next-hop-self

origin

Syntax	origin {igp egp incomplete} no origin
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	This command sets the BGP origin assigned to routes exported into BGP. If the routes are exported into protocols other than BGP, this option is ignored. The no form of the command disables setting the BGP origin for the route policy entry.
Default	no origin
Parameters	igp — sets the path information as originating within the local AS egp — sets the path information as originating in another AS incomplete — sets the path information as learned by some other means

preference

Syntax	preference <i>preference</i> no preference
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	This command assigns a route preference to routes matching the route policy statement entry. If no preference is specified, the default route table manager (RTM) preference for the protocol is used. The no form of the command disables setting an RTM preference in the route policy entry.

Default	no preference
Parameters	<i>preference</i> — the route preference expressed as a decimal integer
Values	1 to 255 (0 represents unset, MIB only)

tag

Syntax	tag <i>hex-string</i> no tag
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	<p>This command assigns an OSPF tag to routes that do not match any entry (for default action) or that match the entry (for action). A hexadecimal value of 4 octets can be entered.</p> <p>The no form of the command removes the tag.</p>
Default	no tag
Parameters	<i>hex-string</i> — assigns an OSPF tag
Values	OSPF: [0x0...0xFFFFFFFF]H

type

Syntax	type <i>type</i> no type
Context	config>router>policy-options>policy-statement>default-action config>router>policy-options>policy-statement>entry>action
Description	<p>This command assigns an OSPF type metric to routes that do not match any entry (for default action) or that match the entry (for action). The no form of the command disables assigning an OSPF type in the route policy entry.</p>
Default	no type
Parameters	<i>type</i> — specifies the OSPF type metric
Values	1 — set as OSPF routes with type 1 LSAs 2 — set as OSPF routes with type 2 LSAs

Show Commands

policy

Syntax	policy [<i>name</i> damping prefix-list <i>name</i> as-path <i>name</i> community <i>name</i> admin]
Context	show>router
Description	This command displays configured policy statement information.
Parameters	<p><i>name</i> — if a name is provided, the matching policy statement is shown. If no statement name is specified, a list of all policies statements and descriptions are shown.</p> <p>damping — displays the damping profile for use in the route policy</p> <p>prefix-list — displays the prefix lists configured in the route policy</p> <p>as-path — displays AS path regular expression statements used in the route policy</p> <p>community — displays community lists used in the route policy</p> <p>admin — if this keyword is included, the entire policy option configuration is shown, including any uncommitted configuration changes. This command is similar to the info command.</p>
Output	<p>The following outputs are examples of route policy information, and Table 42 describes the fields.</p> <ul style="list-style-type: none"> • Sample Output - show router policy • Sample Output - show router policy admin • Sample Output - show router policy name • Sample Output - show router policy damping • Sample Output - show router policy prefix-list • Sample Output - show router policy prefix-list name • Sample Output - show router policy as-path • Sample Output - show router policy as-path name • Sample Output - show router policy community • Sample Output - show router policy community name

Sample Output - show router policy

The **show router policy** command displays all configured route policies.

```
A:ALU-1# show router policy
=====
Route Policies
=====
Policy                               Description
-----
BGP To OSPF                         Policy Statement For 'BGP To OSPF'
Direct And Aggregate                 Policy Statement ABC
-----
Policies : 3
=====
A:ALU-1#
```

Sample Output - show router policy admin

The **show router policy admin** command is similar to the **info** command, which displays information about the route policies and parameters.

```
A:ALU-1# show router policy admin
  prefix-list "All-Routes"
    prefix 0.0.0.0/0 longer
    prefix 2.0.0.0/8 longer
    prefix 3.0.0.0/8 longer
    prefix 4.0.0.0/8 longer
    prefix 5.0.0.0/8 longer
    prefix 6.0.0.0/8 exact
    prefix 224.0.0.0/24 longer
  exit
  community "65206" members "no-export" "no-export-subconfed"
  community "AS65000" members "701:65000"
  as-path "test" "14001 701"
  as-path "test1" "1234{1,6} (56|47) (45001|2000|1534)* 9+"
  damping "TEST-LOW"
    half-life 22
    max-suppress 720
    reuse 10000
    suppress 15000
  exit
  damping "TEST-HIGH"
    half-life 22
    max-suppress 720
    reuse 1000
    suppress 5000
  exit
  damping "TEST-MEDIUM"
    half-life 22
    max-suppress 720
    reuse 5000
    suppress 11000
  exit
  policy-statement "BGP To OSPF"
    description "Policy Statement For 'BGP To OSPF'"
    entry 10
      description "Entry For Policy 'BGP To OSPF'"
  exit
```



```

        from
            protocol bgp
        exit
    to
        protocol rip
    exit
    action accept
        metric set 1
        next-hop 10.0.18.200
        tag 0x8008135
    exit
exit
default-action reject
exit
policy-statement "Direct And Aggregate"
    entry 10
        from
            protocol direct
        exit
        to
            protocol bgp
        exit
        action accept
        exit
    exit
    entry 20
        from
            protocol aggregate
        exit
        to
            protocol bgp
        exit
        action accept
        exit
    exit
exit
...
A:ALU-1#

```

Sample Output - show router policy *name*

The **show router policy *name*** command displays information about a specific route policy.

```

description "Policy Statement For 'BGP To OSPF'"
    entry 10
        description "Entry For Policy 'BGP To OSPF'"
        from
            protocol bgp
        exit
        to
            protocol rip
        exit
        action accept
            metric set 1
            next-hop 10.0.18.200
            tag 0x8008135
        exit
    exit

```

```
default-action reject
A:ALU-1#
```

Sample Output - show router policy damping

The **show router policy damping** command displays information about the route policy damping configurations.

```
A:ALU-1# show router policy damping
=====
Route Damping Profiles
=====
damping "TEST-LOW"
  half-life 22
  max-suppress 720
  reuse 10000
  suppress 15000
exit
damping "TEST-HIGH"
  half-life 22
  max-suppress 720
  reuse 1000
  suppress 5000
exit
damping "TEST-MEDIUM"
  half-life 22
  max-suppress 720
  reuse 5000
  suppress 11000
exit
=====
A:ALU-1#
```

Sample Output - show router policy prefix-list

The **show router policy prefix-list** command displays a list of configured prefix lists.

```
A:ALU-1# show router policy prefix-list
=====
Prefix Lists
=====
Prefix List Name
-----
All-Routes
=====
A:ALU-1#
```

Sample Output - show router policy prefix-list *name*

The **show router policy prefix-list *name*** command displays information about a specific prefix list.

```
A:ALU-1# show router policy prefix-list All-Routes
    prefix 0.0.0.0/0 longer
    prefix 2.0.0.0/8 longer
    prefix 3.0.0.0/8 longer
    prefix 4.0.0.0/8 longer
    prefix 5.0.0.0/8 longer
    prefix 6.0.0.0/8 exact
    prefix 224.0.0.0/24 longer
A:ALU-1#
```

Sample Output - show router policy as-path

The **show router policy as-path** command displays a list of configured AS paths.

```
A:ALU-1# show router policy as-path
=====
AS Paths
=====
AS Path Name
-----
test
test1
-----
AS Paths : 2
=====
A:ALU-1#
```

Sample Output - show router policy as-path *name*

The **show router policy as-path *name*** command displays information about a specific AS path.

```
A:ALU-1# show router policy as-path test
as-path "test" "14001 701"
```

Sample Output - show router policy community

The **show router policy community** command displays a list of configured communities.

```
A:ALU-1# show router policy community
=====
Communities
=====
Community Name
-----
65206
AS701
AS65000
-----
Communities : 3
=====
A:ALU-1#
```

Sample Output - show router policy community *name*

The **show router policy community *name*** command displays information about a specific community.

```
A:ALU-1# show router policy community 65206
community "65206" members "no-export" "no-export-subconfed"
A:ALU-1#
```

Table 42: Show Route Policy Output Fields

Label	Description
Policy	The list of route policy names
Description	The description of each route policy
Policies	The total number of policies configured
Damping	The damping profile name
half-life	The half-life parameter for the route damping profile
max-suppress	The maximum suppression parameter configured for the route damping profile
Prefix List	The prefix list name and IP address/mask and whether the prefix list entry only matches (exact) the route with the specified ip-prefix and prefix mask (length) values or values greater (longer) than the specified mask
AS Path	The list of AS path names
AS Paths	The total number of AS paths configured
Community Name	The list of community names
Communities	The total number of communities configured

Standards and Protocol Support

Standards Compliance

IEEE 802.1ag	Service Layer OAM
IEEE 802.1p/q	VLAN Tagging
IEEE 802.3	10BaseT
IEEE 802.3ah	Ethernet OAM
IEEE 802.3u	100BaseTX
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BaseSX/LX
IEEE 802.3-2008	Revised base standard
ITU-T Y.1731	OAM functions and mechanisms for Ethernet-based networks

Telecom Compliance

IC CS-03 Issue 9	Spectrum Management and Telecommunications
ACTA TIA-968-A	
AS/ACIF S016 (Australia/New Zealand)	Requirements for Customer Equipment for connection to hierarchical digital interfaces
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.712-2001	Transmission performance characteristics of pulse code modulation channels
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
ITU-T V.24	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit- terminating equipment (DCE)
ITU-T V.36	Modems for synchronous data transmission using 60-108 kHz group band circuits
ITU-T X.21	Interface between Data Terminal Equipment and Data Circuit- Terminating Equipment for Synchronous Operation on Public Data Networks

Protocol Support

ATM

RFC 2514	Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
RFC 2515	Definition of Managed Objects for ATM Management, February 1999
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
af-tm-0121.000	Traffic Management Specification Version 4.1, March 1999
ITU-T Recommendation I.610	B-ISDN Operation and Maintenance Principles and Functions version 11/95
ITU-T Recommendation I.432.1	B-ISDN user- network interface - Physical layer specification: General characteristics
GR-1248-CORE	Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
GR-1113-CORE	Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
AF-PHY-0086.001	Inverse Multiplexing for ATM (IMA)

BFD

draft-ietf-bfd-mib-00.txt	Bidirectional Forwarding Detection Management Information Base
draft-ietf-bfd-base-o5.txt	Bidirectional Forwarding Detection
draft-ietf-bfd-v4v6-1hop-06.txt	BFD IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-multihop-06.txt	BFD for Multi-hop Paths

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MDS
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
- RFC 4724 Graceful Restart Mechanism for BGP - GR Helper
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4893 BGP Support for Four-octet AS Number Space

DHCP/DHCPv6

- RFC 1534 Interoperation between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 3315 Dynamic Host Configuration Protocol for IPv6

DIFFERENTIATED SERVICES

- RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

DIGITAL DATA NETWORK MANAGEMENT

- V.35
- RS-232 (also known as EIA/TIA-232)

GRE

- RFC 2784 Generic Routing Encapsulation (GRE)

IPv6

- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 4649 DHCPv6 Relay Agent Remote-ID Option
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)

LDP

- RFC 5036 LDP Specification

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 4205 for Shared Risk Link Group (SRLG) TLV draft-ietf-isis-igp-p2p-over-lan-05.txt
- RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

NETWORK MANAGEMENT

- ITU-T X.721: Information technology- OSI-Structure of Management Information
- ITU-T X.734: Information technology- OSI-Systems Management: Event Report Management Function
- M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- RFC 2571 SNMP-FRAMEWORKMIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASED ACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2588 SONET-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 3014 NOTIFICATION-LOG MIB
- RFC 3164 The BSD Syslog Protocol
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- IANA-IFType-MIB

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF
- RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

PPP

- RFC 1332 PPP Internet Protocol Control Protocol (IPCP)
- RFC 1570 PPP LCP Extensions
- RFC 1619 PPP over SONET/SDH
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 2686 The Multi-Class Extension to Multi-Link PPP

PSEUDOWIRES

- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocation for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
draft-ietf-pwe3-redundancy-02 Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

RSVP-TE and FRR

RFC 2430 A Provider Architecture for DiffServ & TE
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC 2747 RSVP Cryptographic Authentication
RFC 3097 RSVP Cryptographic Authentication - Updated Message Type Value
RFC 3209 Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels
RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

SONET/SDH

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
ITU-T Recommendation G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

SYNCHRONIZATION

G.813 Timing characteristics of SDH equipment slave clocks (SEC)
G.8261 Timing and synchronization aspects in packet networks
G.8262 Timing characteristics of synchronous Ethernet equipment slave clock
GR 1244 CORE Clocks for the Synchronized Network: Common Generic Criteria
IEEE 1588v2 1588 PTP 2008

TACACS+

IETF draft-grant-tacacs-02.txt The TACACS+ Protocol

TCP/IP

RFC 768 User Datagram Protocol
RFC 791 Internet Protocol
RFC 792 Internet Control Message Protocol
RFC 793 Transmission Control Protocol
RFC 826 Ethernet Address Resolution Protocol
RFC 854 Telnet Protocol Specification
RFC 1350 The TFTP Protocol (Rev. 2)
RFC 1812 Requirements for IPv4 Routers

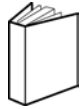
VPLS

RFC 4762 Virtual Private LAN Services Using LDP

Proprietary MIBs

TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/myaccess>

Product manuals and documentation updates are available at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

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



Documentation feedback

documentation.feedback@alcatel-lucent.com

