



Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 3.0
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	25
Getting Started	29
Alcatel-Lucent 7705 SAR Router Configuration Process	29
Notes on 7705 SAR-8 and 7705 SAR-F	30
IP Router Configuration	33
Configuring IP Router Parameters	34
Interfaces	34
Network Interface	34
System Interface	36
IP Addresses	36
Router ID	37
Autonomous Systems (AS)	38
DHCP Relay	38
DHCP Options	39
Static Routes, Dynamic Routes, and ECMP	39
IGP-LDP and Static Route-LDP Synchronization	40
Bidirectional Forwarding Detection (BFD)	41
Router Configuration Process Overview	42
Configuration Notes	43
Reference Sources	43
Configuring an IP Router with CLI	45
Router Configuration Overview	46
System Interface	46
Network Interface	47
Basic Configuration	48
Common Configuration Tasks	49
Configuring a System Name	49
Configuring Interfaces	50
Configuring a System Interface	50
Configuring a Network Interface	50
Configuring ECMP	51
Configuring Static Routes	52
Configuring or Deriving a Router ID	53
Configuring an Autonomous System	54
Configuring DHCP for the Router	54
Service Management Tasks	56
Changing the System Name	56
Modifying Interface Parameters	57
Deleting a Logical IP Interface	58
IP Router Command Reference	59
Command Hierarchies	59
Command Descriptions	64
Configuration Commands	65
Show Commands	87

Table of Contents

Clear Commands	109
Debug Commands	112
Filter Policies	117
Configuring Filter Policies	118
Network and Service Interface-based Filtering	119
Filter Policy Entries	119
Applying Filter Policies	120
Packet Matching Criteria	121
Ordering Filter Entries	122
Filter Logs	125
Configuration Notes	126
IP Filters	126
Filter Logs	126
Reference Sources	127
Configuring Filter Policies with CLI	129
Basic Configuration	130
Common Configuration Tasks	131
Creating an IP Filter Policy	131
IP Filter Policy	131
IP Filter Entry	133
IP Filter Entry Matching Criteria	134
Configuring Filter Log Policies	135
Applying Filter Policies to Network Interfaces	135
Apply a Filter Policy to an Interface	135
Filter Management Tasks	137
Renumbering Filter Policy Entries	137
Modifying an IP Filter Policy	139
Deleting a Filter Policy	140
Deleting a Filter from a Network Interface	140
Deleting a Filter	140
Filter Command Reference	141
Command Hierarchies	141
Command Descriptions	144
Configuration Commands	145
Show Commands	163
Clear Commands	172
Monitor Commands	173
Route Policies	175
Configuring Route Policies	176
Routing Policy and MPLS	176
Policy Statements	177
Default Action Behavior	177
Denied IP Prefixes	178
Controlling Route Flapping	178
Regular Expressions	180
BGP and OSPF Route Policy Support	184
BGP Route Policies	185
Readvertised Route Policies	185

When to Use Route Policies	185
Route Policy Configuration Process Overview	186
Configuration Notes	187
Reference Sources	187
Configuring Route Policies with CLI	189
Route Policy Configuration Overview	190
When to Create Routing Policies	190
Default Route Policy Actions	191
Policy Evaluation	192
Damping	196
Basic Route Policy Configuration	197
Configuring Route Policy Components	199
Beginning the Policy Statement	200
Creating a Route Policy	200
Configuring a Default Action	202
Configuring an Entry	203
Configuring an AS Path (policy-option)	205
Configuring a Community List	205
Configuring Damping	206
Configuring a Prefix List	206
Route Policy Configuration Management Tasks	208
Editing Policy Statements and Parameters	208
Deleting an Entry	209
Deleting a Policy Statement	210
Route Policy Command Reference	211
Command Hierarchies	211
Command Descriptions	214
Configuration Commands	215
Show Commands	239
Standards and Protocol Support	245

List of Tables

Getting Started	29
Table 1: Configuration Process	29
Table 2: 7705 SAR-8 and 7705 SAR-F Comparison	30
IP Router Configuration	33
Table 3: Route Preference Defaults by Route Type	70
Table 4: Show ARP Table Output Fields	88
Table 5: Show Authentication Statistics Output Fields	89
Table 6: Show BFD Interface Output Fields	91
Table 7: Show BFD Session Output Fields	92
Table 8: Show DHCP Statistics Output Fields	93
Table 9: Show DHCP Summary Output Fields	94
Table 10: Show ECMP Settings Output Fields	96
Table 11: Show Standard IP Interface Output Fields	98
Table 12: Show Detailed IP Interface Output Fields	99
Table 13: Show Summary IP Interfaces Output Fields	101
Table 14: Show Standard Route Table Output Fields	102
Table 15: Show Static ARP Table Output Fields	104
Table 16: Show Static Route Table Output Fields	105
Table 17: Show Router Status Output Fields	106
Table 18: Show Tunnel Table Output Fields	108
Filter Policies	117
Table 19: Show Filter Output Fields	164
Table 20: Show Filter Output Fields (Filter ID Specified)	165
Table 21: Show Filter Associations Output Fields	167
Table 22: Show Filter Counters Output Fields	169
Table 23: Show Filter Log Output Fields	170
Table 24: Show Filter Log Bindings	171
Route Policies	175
Table 25: Regular Expression Operators	181
Table 26: AS Path and Community Regular Expression Examples	181
Table 27: Show Route Policy Output Fields	244

List of Figures

IP Router Configuration	33
Figure 1: IP Router Configuration Flow	42
Filter Policies	117
Figure 2: Creating and Applying Filter Policies	121
Figure 3: Filtering Process Example	124
Route Policies	175
Figure 4: BGP Route Policy Diagram	184
Figure 5: OSPF Route Policy Diagram	184
Figure 6: Route Policy Configuration and Implementation Flow	186
Figure 7: Route Policy Process Example	193
Figure 8: Next Policy Logic Example	194
Figure 9: Next Entry Logic Example	195
Figure 10: Damping Example	196

List of Figures

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
A/S	active/standby
ABR	available bit rate area border router
AC	alternating current attachment circuit
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
AS	autonomous system
ASAP	any service, any port

List of Acronyms

Acronym	Expansion
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
BFDD	bidirectional forwarding detection
BGP	border gateway protocol
BITS	building integrated timing supply
BOF	boot options file
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSTA	Broadband Service Termination Architecture
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

Acronym	Expansion
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)
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
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

Acronym	Expansion
DES	data encryption standard
DHCP	dynamic host configuration protocol
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
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
DV	delay variation
e911	enhanced 911 service
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

Acronym	Expansion
E&M	ear and mouth earth and magneto exchange and multiplexer
Epipe	Ethernet VLL
ERO	explicit route object
ESD	electrostatic discharge
ESMC	Ethernet synchronization message channel
ETE	end-to-end
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVDO	evolution - data optimized
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

List of Acronyms

Acronym	Expansion
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
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
IANA	internet assigned numbers authority
IBN	isolated bonding networks
ICMP	Internet control message protocol
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

Acronym	Expansion
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
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LIB	label information base
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

Acronym	Expansion
LTN	LSP ID to NHLFE
LTR	linktrace reply
MA	maintenance association
MA-ID	maintenance association identifier
MAC	media access control
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

Acronym	Expansion
MIP	maintenance association intermediate point
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
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
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
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)

List of Acronyms

Acronym	Expansion
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
PDU	protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PHB	per-hop behavior
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

Acronym	Expansion
PPP	point-to-point protocol
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
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)
RSVP-TE	resource reservation protocol - traffic engineering
R&TTE	Radio and Telecommunications Terminal Equipment

List of Acronyms

Acronym	Expansion
RT	receive/transmit
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
RTU	remote terminal unit
SAA	service assurance agent
SAP	service access point
SAR-8	7705 Service Aggregation Router - 8-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
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
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNTP	simple network time protocol

Acronym	Expansion
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
STM1	synchronous transport module, level 1
SVC	switched virtual circuit
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
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
TTL	time to live
TTM	tunnel table manager
U-APS	unidirectional automatic protection switching
UBR	unspecified bit rate

Acronym	Expansion
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
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
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.

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, contact your welcome center at:

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

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 33
Protocol configuration	Configure IP filters	Filter Policies on page 117
	Configure routing policies	Route Policies on page 175
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 245

Notes on 7705 SAR-8 and 7705 SAR-F

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

The 7705 SAR-8 has an 8-slot chassis that supports two CSMs, a Fan module and six 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 and 7705 SAR-F Comparison

7705 SAR-8	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	
16-port T1/E1 ASAP Adapter card	16 individual T1/E1 ports on the faceplate	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, except that the 16 T1/E1 ports on the 7705 SAR-F support multiple synchronization sources to support two timing references. On the 7705 SAR-8, the CLI indicates the MDA type for the 16-port T1/E1 ASAP Adapter card as <code>a16-chds1</code> . On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F ports as <code>a16-chds1v2</code> .

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

7705 SAR-8	7705 SAR-F	Notes
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 Ethernet ports on the 7705 SAR-F are 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>The +24 VDC version of the 7705 SAR-8 only supports version 2 of the 8-port Ethernet Adapter card.</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-F, the CLI indicates the MDA type for the 7705 SAR-F Ethernet ports as <code>a8-ethv3</code>, to distinguish it from the actual version 2 of the 8-port Ethernet Adapter card.</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 34](#)
 - [Interfaces on page 34](#)
 - [IP Addresses on page 36](#)
 - [Router ID on page 37](#)
 - [Autonomous Systems \(AS\) on page 38](#)
 - [DHCP Relay on page 38](#)
 - [Static Routes, Dynamic Routes, and ECMP on page 39](#)
 - [IGP-LDP and Static Route-LDP Synchronization on page 40](#)
 - [Bidirectional Forwarding Detection \(BFD\) on page 41](#)
- [Router Configuration Process Overview on page 42](#)
- [Configuration Notes on page 43](#)
- [Configuring an IP Router with CLI on page 45](#)
- [IP Router Command Reference on page 59](#)

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 attributes such as an IP address, port, or the system with the IP interface.

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. 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](#)
- [Router ID](#)
- [Autonomous Systems \(AS\)](#)
- [DHCP Relay](#)
- [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 interface type (network and system) and address. A network interface is configured on a port. A system interface is associated with a network entity.

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.

IP support discussed in this document includes control plane messaging (including MPLS signaling, next-hop address resolution, management traffic (SNMP), and for OAM purposes). The 7705 SAR can be used as an LER (label edge router) or LSR (label switch router). In order to switch traffic from one SAR or SR node to another in the network, IP forwarding must also be supported.

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.



Note: 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.

Note: 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.

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/mask_length>` or `<ip_address/subnet mask>`. Only IP version 4 (IPv4) addresses are supported.

Router ID

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

IS-IS and BGP use the router ID as its 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 (AS)

Networks can be grouped into areas. An area is a collection of network segments within an 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: Release 3.0 of the 7705 SAR supports IBGP only; it does not support EBGP.

DHCP Relay

The 7705 SAR provides DHCP/BOOTP Relay agent services for DHCP clients. 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.

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

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

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.

With the introduction of IP forwarding and support of the 7705 SAR as an LSR, ECMP is also used to balance IP traffic. 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.

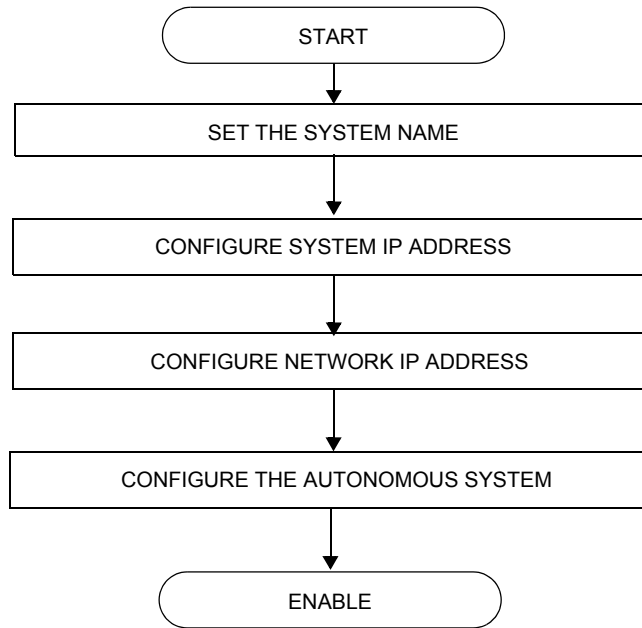
If the configured number of consecutive BFD missed messages is reached, the static route to the peer is declared not active.

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 1 displays the process to configure basic router parameters.

Figure 1: 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 on page 245](#).

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 46](#)
 - [System Interface on page 46](#)
 - [Network Interface on page 47](#)
- [Basic Configuration on page 48](#)
- [Common Configuration Tasks on page 49](#)
 - [Configuring a System Name on page 49](#)
 - [Configuring Interfaces on page 50](#)
 - [Configuring ECMP on page 51](#)
 - [Configuring Static Routes on page 52](#)
 - [Configuring or Deriving a Router ID on page 53](#)
 - [Configuring an Autonomous System on page 54](#)
 - [Configuring DHCP for the Router on page 54](#)
- [Service Management Tasks on page 56](#)
 - [Changing the System Name on page 56](#)
 - [Modifying Interface Parameters on page 57](#)
 - [Deleting a Logical IP Interface on page 58](#)

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 on page 117](#) and [Route Policies on page 175](#) 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 ECMP](#)
- [Configuring Static Routes](#)
- [Configuring or Deriving a Router ID](#)
- [Configuring an Autonomous System](#)
- [Configuring DHCP for the Router](#)

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

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

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: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 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.

With the introduction of IP forwarding and support of the 7705 SAR as an LSR, ECMP is also used to balance IP traffic. 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.

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.

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-in-name | 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: `router-id ip-address`
`interface ip-int-name`
`address {ip-address/mask | ip-address netmask}`

The following displays a router ID configuration example:

```
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 DHCP for the Router

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.

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 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](#)
- [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-int-name | 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**
 - **unreachables** [number seconds]
 - **no unreachables**
- **ingress**
 - **filter ip** ip-filter-id
 - **no filter**
 - **no filter** [ip ip-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

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
    — ecmp
    — fib slot-number [ip-prefix/prefix-length] [longer] [secondary]
    — fib slot-number summary
    — fib slot-number [nh-table-usage]
    — interface [{ip-address | ip-int-name} [detail]] | [summary] | [exclude-services]
    — interface family [detail]
    — isis
    — ldp
```

- **mpls**
- **ospf**
- **policy**
- **route-table** [*family*] [*ip-prefix[/prefix-length]*] [**longer** | **exact**] | [**protocol** *protocol-name*] | [**summary**]
- **rsvp**
- **sgt-qos**
- **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]
- **static-route** [*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**
 - **interface** [*ip-int-name* | *ip-addr*] [**icmp**]
 - **isis**
 - **ldp**
 - **mpls**
 - **ospf**

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
      — [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 on page 175](#).

Command Descriptions

- [Configuration Commands on page 65](#)
- [Show Commands on page 87](#)
- [Clear Commands on page 109](#)
- [Debug Commands on page 112](#)

Configuration Commands

- [Generic Commands on page 66](#)
- [Router Global Commands on page 67](#)
- [Router Interface Commands on page 73](#)
- [Router Interface DHCP Commands on page 81](#)
- [Router Interface Filter Commands on page 84](#)
- [Router Interface ICMP Commands on page 85](#)

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
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	<p><i>router-name</i> — the router name</p> <table> <tr> <td>Values</td> <td>router-name:</td> <td>Base, management</td> </tr> <tr> <td>Default</td> <td></td> <td>Base</td> </tr> </table>	Values	router-name:	Base, management	Default		Base
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 — no aggregate routes are defined						
Parameters	<i>ip-prefix/ip-prefix-length</i> — the destination address of the aggregate route in dotted-decimal notation						
	<table> <tr> <td>Values</td> <td><i>ip-prefix</i></td> <td>a.b.c.d (host bits must be 0)</td> </tr> <tr> <td></td> <td><i>ip-prefix-length</i></td> <td>0 to 32</td> </tr> </table>	Values	<i>ip-prefix</i>	a.b.c.d (host bits must be 0)		<i>ip-prefix-length</i>	0 to 32
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.

ECMP is also used to balance IP traffic. 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 ip-address 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> <p>The no form of the command reverts to the default value.</p>
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	<i>ip-address</i> — 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-int-name | 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 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.
- Default** no static-route
- Parameters** *ip-prefix/prefix-length* — the destination address of the static route
- Values** *ip-prefix* a.b.c.d (host bits must be 0)
ip-prefix-length 0 to 32
- 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 3](#).

Table 3: 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-int-name | *ip-address* — specifies the directly connected next-hop IP address used to reach the destination. If the next hop is over an unnumbered interface, the *ip-int-name* of the unnumbered interface (on this node) can be configured.

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 *ip-int-name* 32 chars max
ip-address a.b.c.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 alphanumeric 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** *seconds*
no ldp-sync-timer

Context config>router>interface

Description This command configures the IGP-LDP synchronization timer to enable synchronization of IGP and LDP and synchronization of static routes and LDP.

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).

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** (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.

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:

- **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**

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.

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.

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	This command enables or disables the receiving of SNTP broadcasts on the IP interface. This parameter is only valid when the SNTP broadcast-client global parameter is configured. The no form of the command disables SNTP broadcast received on the IP interface.
Default	no ntp-broadcast

port

Syntax	port <i>port-name</i> no port																					
Context	config>router>interface																					
Description	<p>This command creates an association with a logical IP interface and a physical port.</p> <p>An interface can also be associated with the system (loopback address).</p> <p>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.</p> <p>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. See the 7705 SAR OS Interface Configuration Guide for information on configuring ports.</p> <p>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.</p>																					
Default	no port																					
Parameters	<i>port-name</i> — the physical port identifier to associate with the IP interface																					
	<table> <tr> <td>Values</td> <td><i>port-id</i></td> <td><i>slot/mda/port</i></td> </tr> <tr> <td></td> <td><i>bundle-id</i></td> <td><i>bundle-type-slot/mda.bundle-num</i></td> </tr> <tr> <td></td> <td></td> <td>bundle keyword</td> </tr> <tr> <td></td> <td></td> <td>type ima, ppp</td> </tr> <tr> <td></td> <td></td> <td>bundle-num 1 to 128</td> </tr> <tr> <td></td> <td><i>encap-val</i></td> <td>0 (for null)</td> </tr> <tr> <td></td> <td></td> <td>0 to 4094 (for dot1q)</td> </tr> </table>	Values	<i>port-id</i>	<i>slot/mda/port</i>		<i>bundle-id</i>	<i>bundle-type-slot/mda.bundle-num</i>			bundle keyword			type ima, ppp			bundle-num 1 to 128		<i>encap-val</i>	0 (for null)			0 to 4094 (for dot1q)
Values	<i>port-id</i>	<i>slot/mda/port</i>																				
	<i>bundle-id</i>	<i>bundle-type-slot/mda.bundle-num</i>																				
		bundle keyword																				
		type ima, ppp																				
		bundle-num 1 to 128																				
	<i>encap-val</i>	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 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	<i>ip-addr</i> — the IP address for the static ARP in IP address dotted-decimal notation <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.

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	This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enters the context for configuring Option 82 suboptions. The no form of this command returns the system to the default.
Default	no option

action

Syntax	action {replace drop keep} no action
Context	config>router>if>dhcp>option
Description	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. The no form of this command returns the system to the default value.
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	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). drop — the packet is dropped, and an error is logged

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 command show>router>interface>detail. 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	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. The no form of this command returns the system to the default.
Default	no remote-id
Parameters	mac — specifies the MAC address of the remote end is encoded in the suboption string <i>string</i> — specifies the remote ID Values up to 32 alphanumeric characters

server

Syntax	server <i>server1</i> [<i>server2</i> ...(up to 8 max)] no server
Context	config>router>if>dhcp
Description	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.
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	This command enables access to the context to configure ingress network filter policies for the IP interface. If an ingress filter is not defined, no filtering is performed.

filter

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



Note: For information on configuring IP filter IDs, see [Creating an IP Filter Policy on page 131](#).

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

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 4](#) 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 4: 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 [*ip-int-name* | *ip-address*]
authentication statistics policy *name*
- Context** show>router>authentication
- Description** This command displays interface or policy authentication statistics.
- Parameters** [*ip-int-name* | *ip-address*] — specifies an existing interface name or IP address
- Values**
- | | |
|--------------------|--------------|
| <i>ip-int-name</i> | 32 chars max |
| <i>ip-address</i> | a.b.c.d |
- name* — specifies an existing policy name
- Output** The following output is an example of the authentication statistics, and [Table 5](#) 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 5: 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 6](#) 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 6: 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 7](#) 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
 12.1.1.2.1        None           5029       5029
net1_2_3           Up (3)         100        100        3
 12.2.3.2          None           156367     156365
-----
No. of BFD sessions: 2
=====
*A:ALU-1#
```

Table 7: 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

statistics

Syntax `statistics [interface ip-int-name | ip-address]`

Context `show>router>dhcp`

Description This command displays statistics for DHCP Relay.

If no IP address or interface name is specified, then all configured interfaces are displayed.

If an IP address or interface name 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 output is an example of DHCP statistics information, and [Table 8](#) describes the fields.

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 8: Show DHCP Statistics Output Fields

Label	Description
DHCP Global Statistics (Service: 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
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

summary

- Syntax** **summary**
- Context** show>router>dhcp
- Description** This command displays a summary of DHCP configuration.
- Output** The following output is an example of DHCP summary information, and [Table 9](#) describes the fields.

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 9: Show DHCP Summary Output Fields

Label	Description
DHCP Summary (Router: Base)	
Interface Name SapID/Sdp	The name of the interface
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

Table 9: Show DHCP Summary Output Fields (Continued)

Label	Description
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

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 10](#) 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 10: 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* [*ip-prefix/prefix-length*] [**longer**] [**secondary**]
fib *slot-number* **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

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

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

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

interface

Syntax **interface** {{{*ip-address* | *ip-int-name*} [**detail**]} | [**summary**] | [**exclude-services**]
interface *family* [**detail**]

Context show>router

Description This command displays the router IP interface table sorted by interface index.

- Parameters**
- ip-address* — only displays the interface information associated with the specified IP address
 - Values** *ip-address* a.b.c.d (host bits must be 0)
 - ip-int-name* — 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

Output The following outputs are examples of IP interface information:

- standard IP interface information ([Sample Output, Table 11](#))
- detailed IP interface information ([Sample Output, Table 12](#))
- summary IP interface information ([Sample Output, Table 13](#))

Sample Output

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

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

Interface-Name IP-Address	Adm	Opr	Mode	Port/SapId PfxState
ip-100.0.0.2 100.10.0.2/10	Up	Down	Network	1/1/1 n/a
system -	Up	Down	Network	system -
to-103 -	Up	Down	Network	n/a -

```
-----
Interfaces : 3
=====
```

```
*A:ALU-1#
```

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

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

Interface-Name IP-Address	Adm	Opr	Mode	Port/SapId PfxState
to-103 -	Up	Down	Network	n/a -

```
-----
```

Table 11: 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	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
Virt. If Index : 3
Last Oper Chg: 04/13/2008 19:35:59
Global If Index : 31
Port Id       : n/a
TOS Marking   : Trusted
If Type       : Network
Egress Filter: none
Ingress Filter : none
SNTP B.Cast   : False
QoS Policy    : 1
MAC Address   :
Arp Timeout   : 14400
IP MTU        : 0
ICMP Mask Reply : True
Arp Populate  : Disabled
LdpSyncTimer  : None
Proxy ARP Details
Rem Proxy ARP: Disabled
Local Proxy ARP : Disabled
Policies      : none
```

```

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 12: 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 Ingress Filter	Indicates whether filters are applied to the port. For Release 3.0, filters are applied to ingress network ports only.
QoS Policy	The QoS policy ID associated with the IP interface
MAC Address	The MAC address of the IP interface

Table 12: Show Detailed IP Interface Output Fields (Continued)

Label	Description
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 13: 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

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

ip-prefix/prefix-length — displays routes only matching the specified IP address and length

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

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 14](#) 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 14: 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

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 15](#) 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 15: 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** [*ip-prefix/prefix-length*] | [**preference** *preference*] | [**next-hop** *ip-address*] | [**tag** *tag*] [**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** *ip-prefix/prefix-length* — displays static routes only matching the specified *ip-prefix* and *prefix-length*
- Values** *ip-prefix* a.b.c.d (host bits must be 0)
prefix-length 0 to 32
- preference* — 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** *ip-address* a.b.c.d (host bits must be 0)
- 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 16](#) 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
   10.200.10.1      to-ser1      1     5   NH   Y
192.168.252.0/24
   10.10.0.254     n/a          1     5   NH   N
192.168.253.0/24
   to-ser1         n/a          1     5   NH   N
=====
A:ALU-A#
```

Table 16: 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.
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 17](#) 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
Total IPv4 Routes 0
ECMP Max Routes  1
Triggered Policies No
=====
*A:ALU-1#
```

Table 17: 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
Total IPv4 Routes	The number of IPv4 routes in the route table

Table 17: Show Router Status Output Fields (Continued)

Label	Description (Continued)
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 18](#) 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 18: 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.

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

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	<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.

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

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	<p><i>ip-int-name</i> — only debugs the specified IP interface</p> <p>Values 32 characters maximum</p> <p><i>ip-address</i> — only debugs the specified IP address</p> <p>Values a.b.c.d</p> <p>headers — only debugs the packet header</p> <p><i>protocol-id</i> — 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.</p> <p>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</p>

route-table

Syntax	route-table [<i>ip-prefix/prefix-length</i>] [longer] no route-table
Context	debug>router>ip
Description	This command configures route table debugging.
Parameters	<i>ip-prefix/prefix-length</i> — the IP prefix for prefix list entry in dotted-decimal notation
Values	<i>ip-prefix</i> a.b.c.d (host bits must be 0) <i>prefix-length</i> 0 to 32
	longer — specifies that the prefix list entry matches any route that matches the specified <i>ip-prefix</i> and <i>prefix-length</i> values greater than the specified <i>prefix-length</i>

Filter Policies

In This Chapter

This chapter provides information about filter policies and management.

Topics in this chapter include:

- [Configuring Filter Policies on page 118](#)
 - [Network and Service Interface-based Filtering on page 119](#)
 - [Filter Policy Entries on page 119](#)
 - [Filter Logs on page 125](#)
- [Configuration Notes on page 126](#)
- [Configuring Filter Policies with CLI on page 129](#)
- [Filter Command Reference on page 141](#)

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), VPRN and IES services, and IES in-band management services. Filter policies constrain network or user traffic based on IP 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 two types of filter policies: IP filters and CSM filters.

In Release 3.0 of the 7705 SAR, IP filters are applied to ingress network interfaces, which affects incoming traffic from the network link, and to ingress IES management SAPs, which affects incoming node management traffic. IP filters are also applied to pseudowire SAPs (Epipes and Ipipes), VPRN SAPs, and IES SAPs, which affects incoming 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.

IP filters scan all traffic and take the appropriate (configured) action against matching packets. Packets that are not filtered by the IP filters and are destined for the 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 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 IP filter policy can be assigned to any entity (network interfaces, IP pseudowires, Ethernet pseudowires, VPRN services, and IES services), all of which can be configured on the same adapter card. For example, a filter policy defined 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.

Up to 16 unique 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 filter policies is similar for network interfaces, IES management SAPs, Ethernet and IP pseudowire SAPs, VPRN SAPs, and IES SAPs. 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 filter policies to SAPs.

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.

Configuring Filter Policies

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

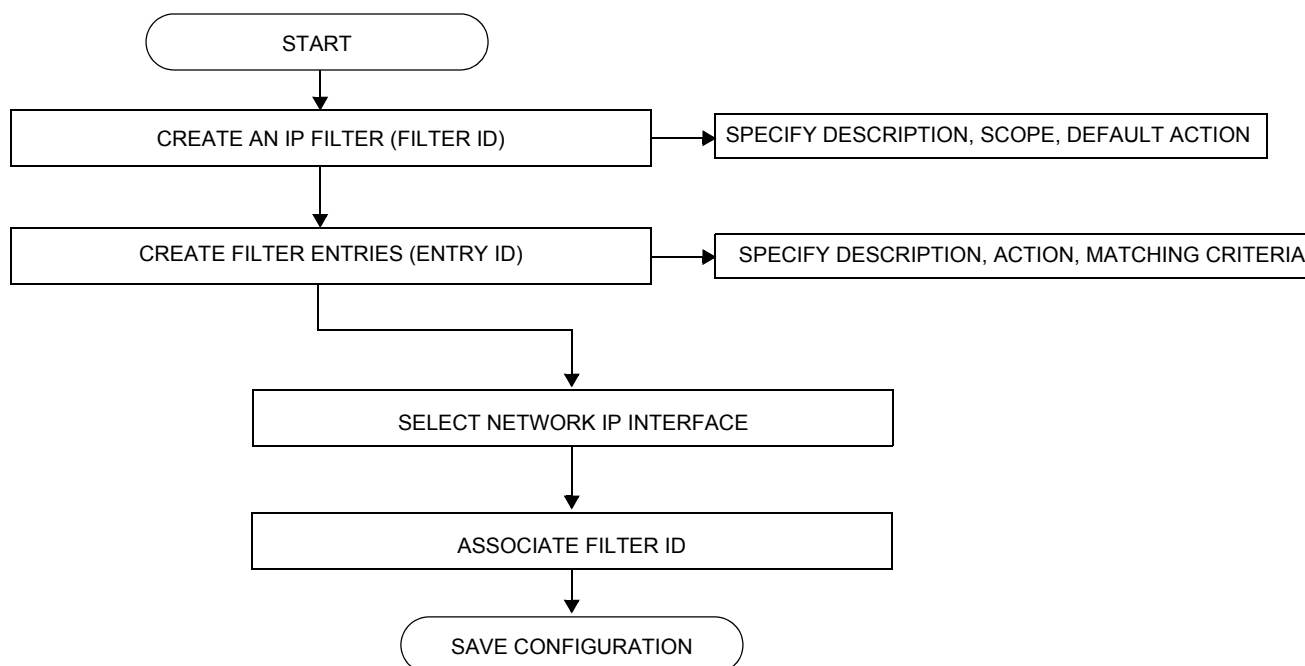
Filter policies can be applied to the ingress of network IP interfaces, Management SAPs, and to the ingress of Ethernet and IP pseudowire SAPs.



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

Figure 2: 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.

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

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.

IP filter policies match criteria that associate traffic with a network interface. Matching criteria to drop or forward IP traffic include:

- protocol identifier — 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).
- DSCP name — matching DiffServ Code Point (DSCP) names
- destination IP address and mask — matching destination IP address and mask values
- destination port/range — matching TCP or UDP values
- fragmentation — matching fragmentation state of packets (fragmented or non-fragmented)
- 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
- multiple IP options — matching state of multiple option fields in the IP header (true or false)
- option present — matching state of the option field in the IP header (present or absent)
- source IP address and mask — matching source IP address and mask values
Address ranges are configured by specifying mask values, the 32-bit combination used to describe the address portion that refers to the subnet and the portion that refers to the host. The mask length is expressed as an integer (range 1 to 32).
- 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)

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).

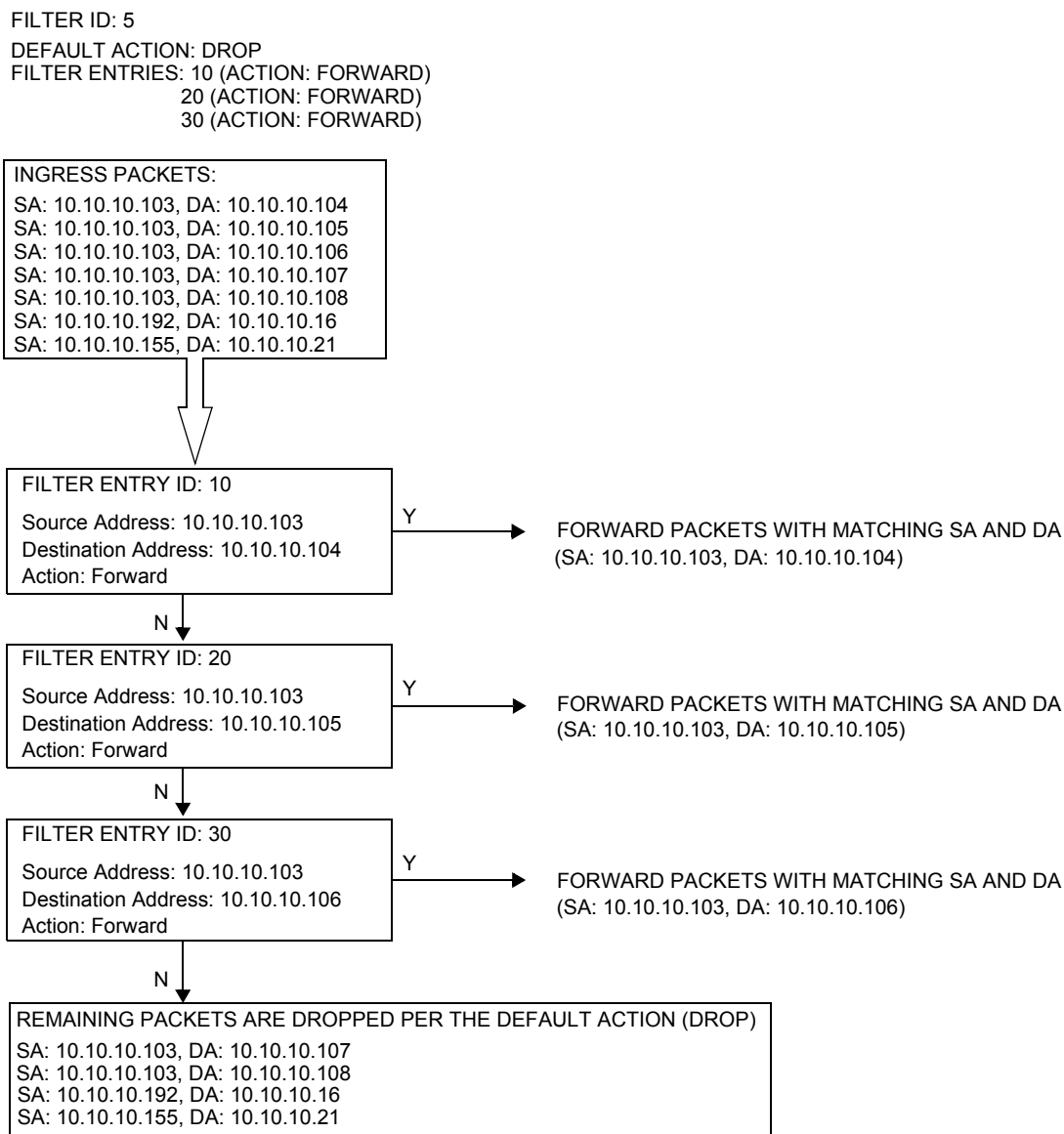
- Packets are compared with the criteria in the first entry ID.
- If a packet matches all the properties defined in the entry, the entry's specified action is executed.
- If a packet does not completely match, the packet continues to the next entry, and then subsequent entries.
- If a packet does not 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 3 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

Figure 3: 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.
- 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 the ingress port or SAP, 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.

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, service filters, or CPM 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 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 on page 245](#).

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 130](#)
- [Common Configuration Tasks on page 131](#)
 - [Creating an IP Filter Policy on page 131](#)
 - [Configuring Filter Log Policies on page 135](#)
 - [Applying Filter Policies to Network Interfaces on page 135](#)
- [Filter Management Tasks on page 137](#)
 - [Renumbering Filter Policy Entries on page 137](#)
 - [Modifying an IP Filter Policy on page 139](#)
 - [Deleting a Filter Policy on page 140](#)

Basic Configuration

The most basic IP 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 IP Filter Policy](#)
- [Configuring Filter Log Policies](#)
- [Applying Filter Policies to Network Interfaces](#)

Creating an IP 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 IP filter policy template:

CLI Syntax: `config>filter# ip-filter filter-id
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`

The following example displays the 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 IP 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

The following example displays the 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 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
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`

The following example displays the 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
exit
-----
A:ALU-7>config>filter>ip-filter#
```

IP Filter Entry Matching Criteria

Use the following CLI syntax to configure IP 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#
```

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 Filter Policies to Network Interfaces

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

Apply a Filter Policy to an Interface

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

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

Common Configuration Tasks

```
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](#)
- [Deleting a Filter Policy](#)

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 filter entries:

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

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

Filter Management Tasks

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 drop
  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 forward
  exit
  exit
...
-----
A:ALU-7>config>filter#
```

Modifying an IP Filter Policy

To access a specific IP 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#
```

The following output displays the 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#
```

Deleting a Filter Policy

Before you can delete a filter, you must remove the filter association from the applied network interfaces.

Deleting a Filter from a Network Interface

To delete a filter from a network interface, enter the following CLI commands:

CLI Syntax: `config>router# interface ip-int-name
ingress
{no filter | no filter ip ip-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 the network interface, use the following CLI syntax to delete the filter.

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

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

Filter Command Reference

Command Hierarchies

- [Configuration Commands](#)
 - [IP Filter Log Configuration Commands](#)
 - [IP Filter Policy Configuration 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
      — description description-string
      — no description
      — default-action {drop | forward}
      — renum old-entry-id new-entry-id
      — scope {exclusive | template}
      — no scope
      — entry entry-id [create]
      — no entry entry-id
        — action [drop]
        — action 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**

Show Commands

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

## Clear Commands

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

Monitor Commands

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

---

## Command Descriptions

- [Configuration Commands on page 145](#)
- [Show Commands on page 163](#)
- [Clear Commands on page 172](#)
- [Monitor Commands on page 173](#)

---

## Configuration Commands

- [Generic Commands on page 146](#)
- [Filter Log Commands on page 147](#)
- [Filter Policy Commands on page 150](#)
- [General Filter Entry Commands on page 152](#)
- [IP Filter Entry Commands on page 153](#)
- [IP Filter Match Criteria Commands on page 156](#)

---

## Generic Commands

### description

|                    |                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>description</b> <i>description-string</i><br><b>no description</b>                                                                                                                                                                                                                         |
| <b>Context</b>     | config>filter>ip-filter<br>config>filter>log<br>config>filter>ip-filter>entry                                                                                                                                                                                                                 |
| <b>Description</b> | This command creates a text description for a configuration context to help identify the content in the configuration file.<br><br>The <b>no</b> form of the command removes any description string from the context.                                                                         |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>description-string</i> — the description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. |

### shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>filter>log<br>config>filter>log>summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | The <b>shutdown</b> 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 <b>no shutdown</b> command.<br><br>Unlike other commands and parameters where the default state is not indicated in the configuration file, <b>shutdown</b> and <b>no shutdown</b> are always indicated in system-generated configuration files.<br><br>The <b>no</b> form of the command puts an entity into the administratively enabled state. |
| <b>Default</b>     | <b>no shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

---

## Filter Log Commands

### log

|                    |                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>log</b> <i>log-id</i> [ <b>create</b> ]<br><b>no log</b> <i>log-id</i>                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>filter                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command enables the context to create a filter log policy.<br><br>The <b>no</b> 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. |

### 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.

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

### destination

|                    |                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>destination memory</b> <i>num-entries</i><br><b>destination syslog</b> <i>syslog-id</i><br><b>no destination</b>                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>filter>log                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures the destination for filter log entries for the specified filter log ID.<br><br>Filter logs can be sent to either memory or an existing syslog server. If the filter log destination is <b>memory</b> , the maximum number of entries in the log must be specified.<br><br>The <b>no</b> form of the command deletes the filter log association. |
| <b>Default</b>     | <b>no destination</b>                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <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.<br><b>Values</b> 1 to 50000                                                                                                                                   |

## Filter Command Reference

*syslog-id* — specifies that the destination of the filter log ID is a syslog server. The *syslog-id* parameter is the identifier of the syslog server.

**Values** 1 to 10

### summary

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

### summary-crit

|                    |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary-crit dst-addr</b><br><b>summary-crit src-addr</b><br><b>no summary-crit</b>                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>filter>log>summary                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command reverts to the default parameter. |
| <b>Default</b>     | <b>dst-addr</b>                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <b>dst-addr</b> — specifies that received log packets are summarized based on the destination IP address<br><b>src-addr</b> — specifies that received log packets are summarized based on the source IP address                                                                                                                                                                                               |

### wrap-around

|                    |                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] wrap-around</b>                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>filter>log                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command configures a memory filter log to store log entries until full or to store the most recent log entries (circular buffer).<br><br>Specifying <b>wrap-around</b> 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. |

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.

**Default**    **wrap-around**

---

## Filter Policy Commands

### ip-filter

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-filter</b> <i>filter-id</i> [ <b>create</b> ]<br><b>no ip-filter</b> <i>filter-id</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>filter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <p>This command creates a configuration context for an IP 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 sub-commands, will be applied immediately to all network interfaces where this policy is applied.</p> <p>The <b>no</b> 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> |
| <b>Parameters</b>  | <i>filter-id</i> — the IP filter policy ID number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Values</b>      | 1 to 65535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                    | <b>create</b> — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the <b>create</b> keyword.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### default-action

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

## renum

|                    |                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>renum</b> <i>old-entry-id</i> <i>new-entry-id</i>                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>filter>ip-filter                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command renumbers existing IP filter entries to properly sequence filter entries.<br><br>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. |
| <b>Parameters</b>  | <i>old-entry-id</i> — the entry number of an existing entry<br><b>Values</b> 1 to 64<br><i>new-entry-id</i> — the new entry number to be assigned to the old entry<br><b>Values</b> 1 to 64                                                                                                                                             |

## scope

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>scope</b> { <b>exclusive</b>   <b>template</b> }<br><b>no scope</b>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>filter>ip-filter                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command configures the filter policy scope as <b>exclusive</b> or <b>template</b> . If the scope of the policy is <b>template</b> and is applied to one or more network interfaces, the scope cannot be changed.<br><br>The <b>no</b> form of the command sets the scope of the policy to the default of <b>template</b> .                                                                                                                                                            |
| <b>Default</b>     | <b>template</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>exclusive</b> — when the scope of a policy is defined as <b>exclusive</b> , 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.<br><br><b>template</b> — when the scope of a policy is defined as <b>template</b> , the policy can be applied to multiple network ports |

---

## General Filter Entry Commands

### entry

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>entry</b> <i>entry-id</i> [ <b>create</b> ]<br><b>no entry</b> <i>entry-id</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>filter>ip-filter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command creates or edits an IP filter entry. Multiple entries can be created using unique <i>entry-id</i> 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 <b>action</b> for it to be considered complete. Entries without the <b>action</b> keyword will be considered incomplete and hence will be rendered inactive.</p> <p>The <b>no</b> form of the command removes the specified entry from the IP filter. Entries removed from the IP filter are immediately removed from all network ports where that filter is applied.</p> |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <p><i>entry-id</i> — an <i>entry-id</i> 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><b>Values</b>      1 to 64</p> <p><b>create</b> — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the <b>create</b> keyword.</p>                                                                                                                                                                                                                                                                                                                                |

---

## IP Filter Entry Commands

### action

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>action [drop]</b><br><b>action [forward]</b><br><b>no action</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>filter>ip-filter>entry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command specifies what action to take (drop or forward) if the packets match the entry criteria. The <b>action</b> 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 <b>no</b> form of the command removes the specified <b>action</b> statement. The filter entry is considered incomplete and is rendered inactive without the <b>action</b> keyword.</p> |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <p><b>drop</b> — specifies that packets matching the entry criteria will be dropped</p> <p><b>forward</b> — 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

|                    |                                                                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>log log-id</b><br><b>no log</b>                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>filter>ip-filter>entry                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command creates 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 <b>no</b> form of the command disables logging for the filter entry.</p> |
| <b>Default</b>     | <b>no log</b>                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <p><i>log-id</i> — the filter log ID destination expressed as a decimal integer</p> <p><b>Values</b> 101 to 199</p>                                                                                                                                                                                                 |

## match

- Syntax** `match [protocol protocol-id]`  
**no match**
- Context** `config>filter>ip-filter>entry`
- Description** This command enables the context to enter match criteria for the filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.
- If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.
- A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.
- The **no** form of the command removes the match criteria for the *entry-id*.
- Parameters** **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.
- protocol-id* — 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.
- Values** 0 to 255 (values can be expressed in decimal, hexadecimal, or binary - DHB)  
 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

| Protocol   | Protocol ID | Description                  |
|------------|-------------|------------------------------|
| icmp       | 1           | Internet Control Message     |
| igmp       | 2           | Internet Group Management    |
| ip         | 4           | IP in IP (encapsulation)     |
| tcp        | 6           | Transmission Control         |
| egp        | 8           | Exterior Gateway Protocol    |
| igp        | 9           | Any private interior gateway |
| udp        | 17          | User Datagram                |
| rdp        | 27          | Reliable Data Protocol       |
| ipv6       | 41          | IPv6                         |
| ipv6-route | 43          | Routing Header for IPv6      |
| ipv6-frag  | 44          | Fragment Header for IPv6     |

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

---

## IP Filter Match Criteria Commands

### dscp

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

|                    |                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-ip</b> { <i>ip-address/mask</i>   <i>ip-address netmask</i> }<br><b>no dst-ip</b>                                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures a destination IP address range to be used as an IP filter match criterion.<br><br>To match on the destination IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.<br><br>The <b>no</b> form of the command removes the destination IP address match criterion. |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>ip-address</i> — the IP prefix for the IP match criterion in dotted-decimal notation<br><br><b>Values</b> 0.0.0.0 to 255.255.255.255<br><br><i>mask</i> — the subnet mask length expressed as a decimal integer<br><br><b>Values</b> 0 to 32                                                                                                                                           |

*netmask* — any mask expressed in dotted-decimal notation

**Values** 0.0.0.0 to 255.255.255.255

## dst-port

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

## fragment

|                    |                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>fragment</b> { <b>true</b>   <b>false</b> }<br><b>no fragment</b>                                                                                                   |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                    |
| <b>Description</b> | This command configures fragmented or non-fragmented IP packets as an IP filter match criterion.<br><br>The <b>no</b> form of the command removes the match criterion. |
| <b>Default</b>     | false                                                                                                                                                                  |

- Parameters** **true** — configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.
- false** — configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

### icmp-code

- Syntax** **icmp-code** *icmp-code*  
**no icmp-code**
- Context** config>filter>ip-filter>entry>match
- Description** This command configures matching on an ICMP code field in the ICMP header of an IP packet as a filter match criterion.
- This option is only meaningful if the protocol match criteria specifies ICMP (1).
- The **no** form of the command removes the criterion from the match entry.
- Default** **no icmp-code**
- Parameters** *icmp-code* — the ICMP code values that must be present to match
- 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

### icmp-type

- Syntax** **icmp-type** *icmp-type*  
**no icmp-type**
- Context** config>filter>ip-filter>entry>match
- Description** This command configures matching on the ICMP type field in the ICMP header of an IP packet as a filter match criterion.
- This option is only meaningful if the protocol match criteria specifies ICMP (1).
- The **no** form of the command removes the criterion from the match entry.
- Default** **no icmp-type**
- Parameters** *icmp-type* — 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** *ip-option-value* [*ip-option-mask*]  
**no ip-option**

**Context** config>filter>ip-filter>entry>match

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

The option type octet contains 3 fields:

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

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

**Default** **no ip-option**

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

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

**Values** 0 to 255

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

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

| Format Style | Format Syntax | Example   |
|--------------|---------------|-----------|
| Decimal      | DDD           | 20        |
| Hexadecimal  | 0xHH          | 0x14      |
| Binary       | 0BBBBBBBB     | 0b0010100 |

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

**Values** 0 to 255

### multiple-option

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

### option-present

|                    |                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>option-present {true   false}</b><br><b>no option-present</b>                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | <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 <b>no</b> form of the command removes the checking of the option field in the IP header as a match criterion.</p>                                                                                |
| <b>Parameters</b>  | <b>true</b> — 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.<br><b>false</b> — specifies matching on IP packets that do not have any option field present in the IP header (an option field of 0) |

### src-ip

|                    |                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-ip {ip-address/mask   ip-address netmask}</b><br><b>no src-ip</b>                                                                                                                                                                                                                  |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command configures a source IP 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> |

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

**Default** **no src-ip**

**Parameters** *ip-address* — the IP prefix for the IP match criterion in dotted-decimal notation

**Values** 0.0.0.0 to 255.255.255.255

*mask* — the subnet mask length expressed as a decimal integer

**Values** 0 to 32

*netmask* — any mask expressed in dotted-decimal notation

**Values** 0.0.0.0 to 255.255.255.255

## src-port

**Syntax** **src-port** {**lt** | **gt** | **eq**} *src-port-number*  
**src-port range** *start end*  
**no src-port**

**Context** config>filter>ip-filter>entry>match

**Description** This command configures a source TCP or UDP port number or port range for an IP filter match criterion.

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

**Default** **no src-port**

**Parameters** **lt** | **gt** | **eq** — use relative to *src-port-number* for specifying the port number match criteria:

**lt** specifies that all port numbers less than *src-port-number* match

**gt** specifies that all port numbers greater than *src-port-number* match

**eq** specifies that *src-port-number* must be an exact match

*src-port-number* — the source port number to be used as a match criteria expressed as a decimal integer

**Values** 1 to 65535

*start end* — specifies an inclusive range of port numbers to be used as a match criteria. The destination port numbers *start* and *end* are expressed as decimal integers.

**Values** 1 to 65535

### tcp-ack

|                    |                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-ack {true   false}</b><br><b>no tcp-ack</b>                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                                                                                                                                  |
| <b>Description</b> | <p>This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.</p> <p>The <b>no</b> form of the command removes the criterion from the match entry.</p>                                |
| <b>Default</b>     | <b>no tcp-ack</b>                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <p><b>true</b> — 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><b>false</b> — 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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-syn {true   false}</b><br><b>no tcp-syn</b>                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>filter>ip-filter>entry>match                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <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 <b>no</b> form of the command removes the criterion from the match entry.</p> |
| <b>Default</b>     | <b>no tcp-syn</b>                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <p><b>true</b> — specifies matching on IP packets that have the SYN bit set in the control bits of the TCP header</p> <p><b>false</b> — 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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip</b> [ <i>ip-filter-id</i> ] [ <b>entry</b> <i>entry-id</i> ] [ <b>association</b>   <b>counters</b> ]                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | show>filter                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command displays IP filter information.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <i>ip-filter-id</i> — displays detailed information for the specified filter ID and its filter entries<br><b>Values</b> 1 to 65535<br><i>entry-id</i> — displays information on the specified filter entry ID for the specified filter ID only<br><b>Values</b> 1 to 64<br><b>association</b> — appends information as to where the filter policy ID is applied to the detailed filter policy ID output<br><b>counters</b> — displays counter information for the specified filter ID |
| <b>Output</b>      | The following outputs are examples of IP filter information: <ul style="list-style-type: none"><li>• IP filter information (<a href="#">Sample Output, Table 19</a>)</li><li>• IP filter information with filter ID specified (<a href="#">Sample Output, Table 20</a>)</li><li>• IP filter associations (<a href="#">Sample Output, Table 21</a>)</li><li>• IP filter counters (<a href="#">Sample Output, Table 22</a>)</li></ul>                                                   |

**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#
```

**Table 19: 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#

```

**Table 20: 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 – indicates the filter is an IP 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. |

**Table 20: Show Filter Output Fields (Filter ID Specified) (Continued)**

| <b>Label</b> | <b>Description</b>                                                                                                                                                                                             |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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                                                                                                                                                   |
| ICMP Type    | The ICMP type match criterion. Undefined indicates no ICMP type specified.                                                                                                                                     |
| 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 Inactive, 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                                                                                                                                                           |
| ICMP Code    | The ICMP code field in the ICMP 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#

```

**Table 21: 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                                 |
| (Ingress)   | The filter policy ID is applied as an ingress filter policy on the interface                                                            |
| Entry       | The filter entry ID. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete as no action was specified. |

**Table 21: Show Filter Associations Output Fields (Continued)**

| Label        | Description                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                       |
| ICMP Type    | The ICMP type match criterion. Undefined indicates no ICMP type 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 – 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                                                                                                                                                     |
| ICMP Code    | The ICMP code field in the ICMP 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#
```

Table 22: 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 IP 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.

**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 23](#))
- filter log bindings ([Sample Output, Table 24](#))

## 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 23: 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 24: 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 or IP                                         |
| 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    |

## Clear Commands

### ip

|                    |                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip</b> <i>ip-filter-id</i> [ <b>entry</b> <i>entry-id</i> ] [ <b>ingress</b>   <b>egress</b> ]                                                                                                                                                                                                                                                                |
| <b>Context</b>     | clear>filter                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>This command clears the counters associated with the IP 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>                                                                                                    |
| <b>Default</b>     | <b>clears all counters associated with the IP filter policy entries</b>                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <p><i>ip-filter-id</i> — the IP filter policy ID</p> <p><b>Values</b> 1 to 65535</p> <p><i>entry-id</i> — only the counters associated with the specified filter policy entry will be cleared</p> <p><b>Values</b> 1 to 64</p> <p><b>ingress</b> — only the ingress counters will be cleared</p> <p><b>egress</b> — only the egress counters will be cleared</p> |

### log

|                    |                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>log</b> <i>log-id</i>                                                                                                                         |
| <b>Context</b>     | clear>filter                                                                                                                                     |
| <b>Description</b> | This command clears the entries associated with the specified filter log. The clear command applies only to logs whose destination is to memory. |
| <b>Parameters</b>  | <p><i>log-id</i> — the filter log ID destination expressed as a decimal integer</p> <p><b>Values</b> 101 to 199</p>                              |

---

## Monitor Commands

### filter

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>filter ip</b> <i>ip-filter-id</i> <b>entry</b> <i>entry-id</i> [ <b>interval</b> <i>seconds</i> ] [ <b>repeat</b> <i>repeat</i> ] [ <b>absolute</b>   <b>rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | monitor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | This command monitors the counters associated with the IP filter policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <i>ip-filter-id</i> — the IP filter policy ID<br><b>Values</b> 1 to 65535<br><i>entry-id</i> — only the counters associated with the specified filter policy entry will be monitored<br><b>Values</b> 1 to 64<br><i>seconds</i> — configures the interval for each display in seconds<br><b>Values</b> 3 to 60<br><b>Default</b> 5<br><i>repeat</i> — configures how many times the command is repeated<br><b>Values</b> 1 to 999<br><b>Default</b> 10<br><b>absolute</b> — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.<br><b>rate</b> — the rate-per-second for each statistic is displayed instead of the delta |



# Route Policies

---

## In This Chapter

This chapter provides information about configuring route policies.

Topics in this chapter include:

- [Configuring Route Policies on page 176](#)
  - [Routing Policy and MPLS on page 176](#)
  - [Policy Statements on page 177](#)
    - [Default Action Behavior on page 177](#)
    - [Denied IP Prefixes on page 178](#)
    - [Controlling Route Flapping on page 178](#)
  - [Regular Expressions on page 180](#)
  - [BGP and OSPF Route Policy Support on page 184](#)
    - [BGP Route Policies on page 185](#)
    - [Readvertised Route Policies on page 185](#)
  - [When to Use Route Policies on page 185](#)
- [Route Policy Configuration Process Overview on page 186](#)
- [Configuration Notes on page 187](#)
- [Configuring Route Policies with CLI on page 189](#)
- [Route Policy Command Reference on page 211](#)

# 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 on page 196](#) 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 25](#).

**Table 25: 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 26](#).

**Table 26: 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<br>11 11<br>11 11<br>11 11 ... 11 |

**Table 26: 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<br>11 22 33 400 500 600                                                                                    |
| Path of any length that ends with AS numbers 44, 55, 66                                                                                           | .* 44 55 66                                | 44 55 66<br>100 44 55 66<br>100 200 44 55 66<br>100 200 300 44 55 66<br>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<br>100 200 33 33<br>100 200 33 33 33<br>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<br>11 11 22 33<br>11 11 22 22 33<br>11 11 22 22 33 33<br>11 ... 11 22 ... 22 33 ...33                      |
| Path whose second AS number must be 11 or 22                                                                                                      | (. 11)   (. 22) .*<br>or<br>. (11   22) .* | 100 11<br>200 22 300 400<br>...                                                                                     |
| Path of length one or two whose second AS number might be 11 or 22                                                                                | . (11   22)?                               | 100<br>200 11<br>300 22                                                                                             |
| Path whose first AS number is 100 and second AS number is either 11 or 22                                                                         | 100 (11   22) .*                           | 100 11<br>100 22 200 300                                                                                            |
| AS path 11, 22, or 33                                                                                                                             | [11 22 33]                                 | 11<br>22<br>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<br>10 10 or 10 11 or 10 12<br>11 10 or 11 11 or 11 12<br>12 10 or 12 11 or 12 12<br>... |
| Zero or one occurrence of AS number 11                                                                                                            | 11? or 11{0,1}                             | Null AS path<br>11                                                                                                  |

Table 26: 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<br>11 11<br>11 11 11<br>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<br>11 11 22<br>11 11 11 22<br>11 11 11 11 22 |
| Path of any length, except nonexistent, whose second AS number can be anything, including nonexistent | . .* or . .{0,}             | 100<br>100 200<br>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<br>22:100<br>11:200<br>...                  |
| AS number is 11 and community value is any number that starts with 1                                  | ^11:(1.*)\$                 | 11:1<br>11:100<br>11:1100                          |
| AS number is any number and community value is any number that ends with 1, 2, or 3                   | ^(.*):(.*[1-3])\$           | 11:1<br>100:2002<br>333:55553<br>...               |
| 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<br>22:3335<br>11:3777779<br>...              |
| AS number is 11 or 22 and community value ends in 33 or 44                                            | [^((11 22)):(.*(33) (44))\$ | 11:33<br>22:99944<br>22:555533<br>...              |
| <b>Note:</b><br>1. The null keyword matches an empty AS path.                                         |                             |                                                    |

## BGP and OSPF Route Policy Support

BGP and OSPF require route policy support. Figure 4 and Figure 5 show how route policies are evaluated in each protocol. Figure 4 depicts BGP support, which applies a route policy as an internal part of the BGP route selection process. Figure 5 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 4: BGP Route Policy Diagram

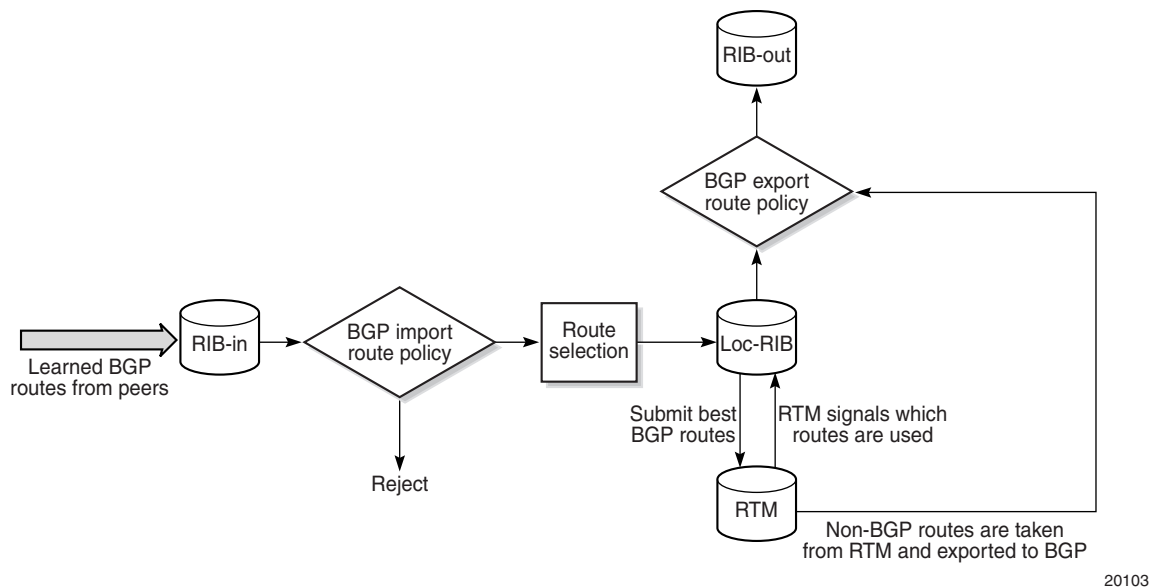
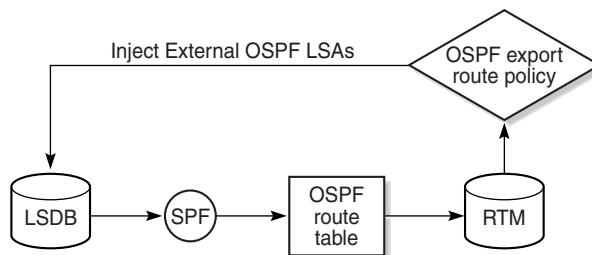


Figure 5: OSPF Route Policy Diagram



20104

## 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

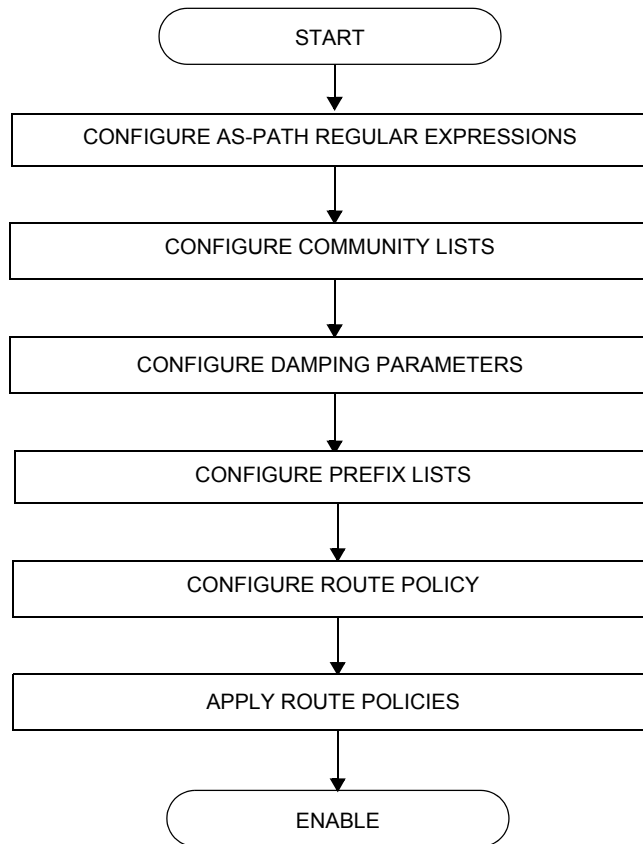
The following are examples of when to configure and apply unique route policies:

- 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 6 displays the process to provision basic route policy parameters.

Figure 6: 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 on page 245](#).

---



## 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 190](#)
  - [When to Create Routing Policies on page 190](#)
  - [Default Route Policy Actions on page 191](#)
  - [Policy Evaluation on page 192](#)
- [Basic Route Policy Configuration on page 197](#)
- [Configuring Route Policy Components on page 199](#)
  - [Beginning the Policy Statement on page 200](#)
  - [Creating a Route Policy on page 200](#)
  - [Configuring a Default Action on page 202](#)
  - [Configuring an Entry on page 203](#)
  - [Configuring an AS Path \(policy-option\) on page 205](#)
  - [Configuring a Community List on page 205](#)
  - [Configuring Damping on page 206](#)
  - [Configuring a Prefix List on page 206](#)
- [Route Policy Configuration Management Tasks on page 208](#)
  - [Editing Policy Statements and Parameters on page 208](#)
  - [Deleting an Entry on page 209](#)
  - [Deleting a Policy Statement on page 210](#)

## 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 3.0 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.

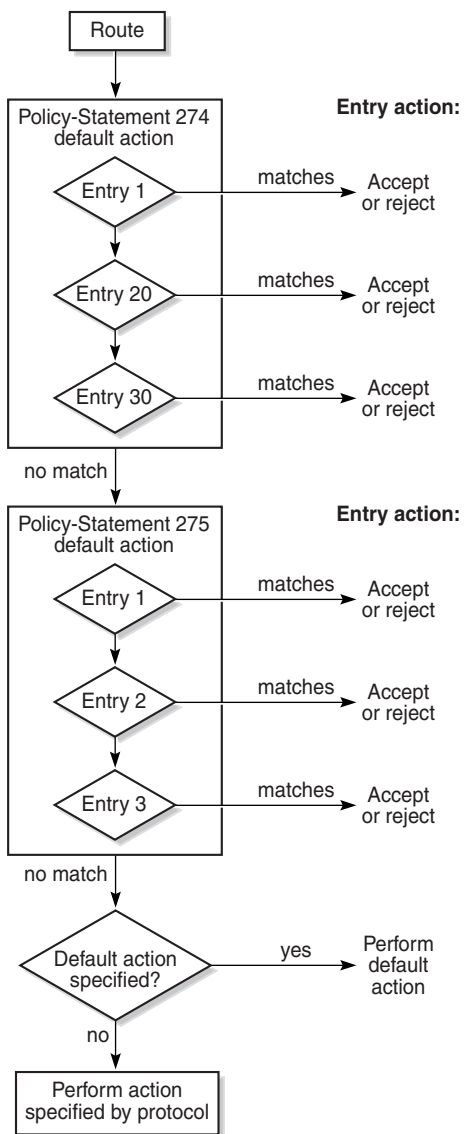
- The process stops when the first complete match is found and executes the action defined in the entry.
- If the packet does not match any of the entries, the system executes the default action specified in the policy statement.

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 7](#) shows an example of the route policy process.

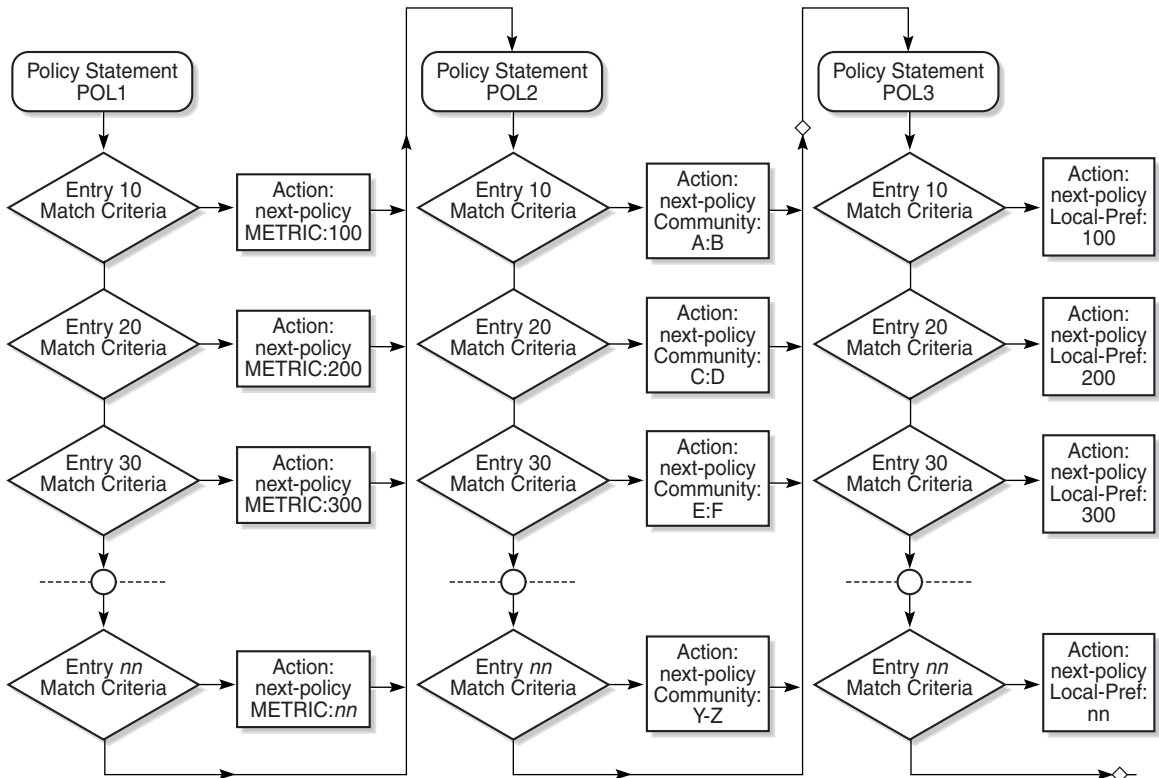
[Figure 8](#) and [Figure 9](#) show the next-policy and next-entry route policy processes.

**Figure 7: Route Policy Process Example**



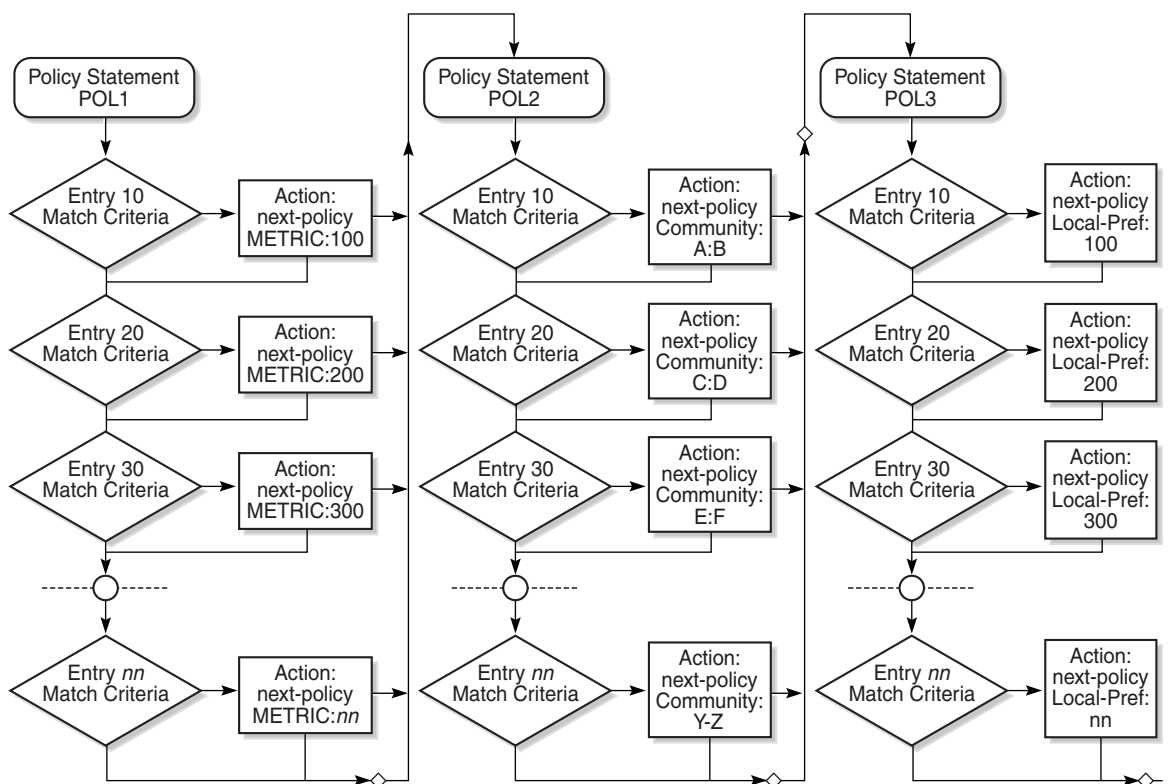
20096

Figure 8: Next Policy Logic Example



20099

Figure 9: 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.

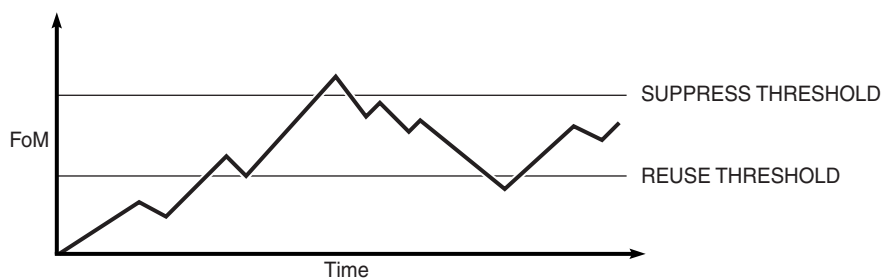
A route can be suppressed according to the Figure of Merit (FoM) value. The FoM is a value that is added to a route each time it flaps. A new route begins with an FoM value of 0.

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 10](#) 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 10: 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
```

## Basic Route Policy Configuration

```
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
```

## Configuring Route Policy Components

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 10 on page 196](#)).
- 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 215](#)
- [Show Commands on page 239](#)

---

## Configuration Commands

- [Generic Commands on page 216](#)
- [Route Policy Options on page 218](#)
- [Route Policy Damping Commands on page 221](#)
- [Route Policy Prefix Commands on page 224](#)
- [Route Policy Entry Match Commands on page 225](#)
- [Route Policy Action Commands on page 232](#)

---

## Generic Commands

### abort

|                    |                                                       |
|--------------------|-------------------------------------------------------|
| <b>Syntax</b>      | <b>abort</b>                                          |
| <b>Context</b>     | config>router>policy-options                          |
| <b>Description</b> | This command discards changes made to a route policy. |
| <b>Default</b>     | none                                                  |

### begin

|                    |                                                                |
|--------------------|----------------------------------------------------------------|
| <b>Syntax</b>      | <b>begin</b>                                                   |
| <b>Context</b>     | config>router>policy-options                                   |
| <b>Description</b> | This command enters the mode to create or edit route policies. |
| <b>Default</b>     | none                                                           |

### commit

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>commit</b>                                      |
| <b>Context</b>     | config>router>policy-options                       |
| <b>Description</b> | This command saves changes made to a route policy. |
| <b>Default</b>     | none                                               |

## description

|                    |                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>description</b> <i>description-string</i><br><b>no description</b>                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options>policy-statement<br>config>router>policy-options>policy-statement>entry                                                                                                                                                                                          |
| <b>Description</b> | <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 <b>no</b> form of the command removes the string from the configuration.</p>                                                                      |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>description-string</i> — the description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes. |

---

## Route Policy Options

### as-path

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>as-path</b> <i>name</i> { <i>regular-expression</i>   <b>null</b> }<br><b>no as-path</b> <i>name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>router>policy-options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | This command creates a route policy AS path regular expression statement to use in route policy entries.<br><br>The <b>no</b> form of the command deletes the AS path regular expression statement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Default</b>     | <b>no as-path</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <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.<br><br><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.<br><br><b>null</b> — the AS path expressed as an empty regular expression string |

### community

|                    |                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>community</b> <i>name</i> <b>members</b> <i>comm-id</i> [ <i>comm-id</i> ...(up to 15 max)]<br><b>no community</b> <i>name</i> [ <b>members</b> <i>comm-id</i> ]                                                                                                    |
| <b>Context</b>     | config>router>policy-options                                                                                                                                                                                                                                           |
| <b>Description</b> | This command creates a route policy community list to use in route policy entries.<br><br>The <b>no</b> form of the command deletes the community list or the provided community ID.                                                                                   |
| <b>Default</b>     | <b>no community</b>                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <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

|                    |                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] policy-options</b>                                                                                                                                                                         |
| <b>Context</b>     | config>router                                                                                                                                                                                      |
| <b>Description</b> | This command enables the context to configure route policies. Route policies are applied to the routing protocol.<br><br>The <b>no</b> form of the command deletes the route policy configuration. |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                        |

### policy-statement

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] policy-statement</b> <i>name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>router>policy-options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <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 <b>policy-statement</b> is a logical grouping of match and action criteria. A single <b>policy-statement</b> can affect routing in one or more protocols and/or one or more protocols' peers/neighbors. A single <b>policy-statement</b> can also affect the export of routing information.</p> <p>The <b>no</b> form of the command deletes the policy statement.</p> |
| <b>Default</b>     | <b>no policy-statement</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] triggered-policy</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <p>This command triggers route policy re-evaluation.</p> <p>By default, when a change is made to a policy in the <b>config router policy-options</b> 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 <b>triggered-policy</b> 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 <b>clear</b> command with the <b>soft</b> or <b>soft-inbound</b> option must be used. In other words, when a <b>triggered-policy</b> is enabled, any routine policy change or policy assignment change within the protocol will not take effect until the protocol is reset or a <b>clear</b> command is issued to re-evaluate route policies; for example, <b>clear router bgp neighbor x.x.x.x soft</b>. This keeps the peer up, and the change made to a route policy is applied only to that peer, or group of peers.</p> |
| <b>Default</b>     | <b>disabled</b> — dynamic route policy is enabled; policy-option configuration changes take effect immediately                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

---

## Route Policy Damping Commands

### damping

|                    |                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] damping</b> <i>name</i>                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options                                                                                                                                                                                                                                            |
| <b>Description</b> | This command creates a context to configure a route damping profile to use in route policy entries.<br><br>The <b>no</b> form of the command deletes the named route damping profile.                                                                                   |
| <b>Default</b>     | <b>no damping</b>                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>half-life</b> <i>minutes</i><br><b>no half-life</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>router>policy-options>damping                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures the half-life parameter for the route damping profile.<br><br>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).<br><br>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 <b>no</b> form of the command removes the half-life parameter from the damping profile. |
| <b>Default</b>     | <b>no half-life</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>minutes</i> — the half-life in minutes expressed as a decimal integer<br><br><b>Values</b> 1 to 45                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

### max-suppress

|                    |                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>max-suppress</b> <i>minutes</i><br><b>no max-suppress</b>                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options>damping                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <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 <b>no</b> form of the command removes the maximum suppression parameter from the damping profile.</p> |
| <b>Default</b>     | <b>no max-suppress</b>                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>minutes</i> — the maximum suppression time, in minutes, expressed as a decimal integer                                                                                                                                                                                                                            |
| <b>Values</b>      | 1 to 720                                                                                                                                                                                                                                                                                                             |

### reuse

|                    |                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>reuse</b> <i>integer</i><br><b>no reuse</b>                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>router>policy-options>damping                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | <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 <b>no</b> form of the command removes the reuse parameter from the damping profile.</p> |
| <b>Default</b>     | <b>no reuse</b>                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>integer</i> — the reuse value expressed as a decimal integer                                                                                                                                                                                                                                                                                               |
| <b>Values</b>      | 1 to 20000                                                                                                                                                                                                                                                                                                                                                    |

## suppress

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>suppress</b> <i>integer</i><br><b>no suppress</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>router>policy-options>damping                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <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 <b>no</b> form of the command removes the suppress parameter from the damping profile.</p> |
| <b>Default</b>     | <b>no suppress</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <i>integer</i> — the suppress value expressed as a decimal integer                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                    | <b>Values</b> 1 to 20000                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

---

## Route Policy Prefix Commands

### prefix-list

|                    |                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] prefix-list</b> <i>name</i>                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>router>policy-options                                                                                                                                                                                                                                        |
| <b>Description</b> | This command creates a context to configure a prefix list to use in route policy entries.<br><br>The <b>no</b> form of the command deletes the named prefix list.                                                                                                   |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |       |                               |  |                     |         |               |         |               |                                                                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------|-------------------------------|--|---------------------|---------|---------------|---------|---------------|-----------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] prefix</b> <i>ip-prefix/prefix-length</i> [ <b>exact</b>   <b>longer</b>   <b>through</b> <i>length</i>   <b>prefix-length-range</b> <i>length1-length2</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                               |       |                               |  |                     |         |               |         |               |                                                                 |
| <b>Context</b>     | config>router>policy-options>prefix-list                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |       |                               |  |                     |         |               |         |               |                                                                 |
| <b>Description</b> | This command creates a prefix entry in the route policy prefix list.<br><br>The <b>no</b> form of the command deletes the prefix entry from the prefix list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                               |       |                               |  |                     |         |               |         |               |                                                                 |
| <b>Parameters</b>  | <i>ip-prefix/prefix-length</i> — the IP prefix for the prefix list entry in dotted-decimal notation <table> <tr> <td><b>Values</b></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><b>exact</b> — the prefix list entry only matches the route with the specified <i>ip-prefix</i> and <i>prefix-length</i> values</p> <p><b>longer</b> — 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><b>Values</b></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><b>Values</b></td> <td>0 to 32, <i>length2</i> &gt; <i>length1</i> &gt; <i>prefix-length</i></td> </tr> </table> | <b>Values</b>                 | ipv4: | a.b.c.d (host bits must be 0) |  | ipv4-prefix-length: | 0 to 32 | <b>Values</b> | 0 to 32 | <b>Values</b> | 0 to 32, <i>length2</i> > <i>length1</i> > <i>prefix-length</i> |
| <b>Values</b>      | ipv4:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | a.b.c.d (host bits must be 0) |       |                               |  |                     |         |               |         |               |                                                                 |
|                    | ipv4-prefix-length:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0 to 32                       |       |                               |  |                     |         |               |         |               |                                                                 |
| <b>Values</b>      | 0 to 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                               |       |                               |  |                     |         |               |         |               |                                                                 |
| <b>Values</b>      | 0 to 32, <i>length2</i> > <i>length1</i> > <i>prefix-length</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |       |                               |  |                     |         |               |         |               |                                                                 |

---

## Route Policy Entry Match Commands

### entry

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>entry</b> <i>entry-id</i><br><b>no entry</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>router>policy-options>policy-statement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <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 <b>no</b> form of the command removes the specified entry from the route policy statement.</p> |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <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><b>Values</b>      1 to 4294967295</p>                                                                                                                                                                                                                                                                                              |

### from

|                    |                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] from</b>                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <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 <b>no</b> form of the command deletes the source match criteria for the route policy statement entry.</p> |

to

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] to</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <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 <b>to</b> command context only applies to export policies. If it is used for an import policy, match criteria is ignored.</p> <p>The <b>no</b> form of the command deletes export match criteria for the route policy statement entry.</p> |

area

|                    |                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>area</b> <i>area-id</i><br><b>no area</b>                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry>from                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <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 <b>no</b> form of the command removes the OSPF area match criterion.</p> |
| <b>Default</b>     | <b>none</b>                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <i>area-id</i> — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer                                                                                                                                                                                                                                                                |
| <b>Values</b>      | 0.0.0.0 to 255.255.255.255 (dotted-decimal), 0 to 4294967295 (decimal)                                                                                                                                                                                                                                                                                               |

as-path

|                    |                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>as-path</b> <i>name</i><br><b>no as-path</b>                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry>from                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <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 (<b>config&gt;router&gt;policy-options&gt;as-path</b> <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.

## Route Policy Command Reference

- 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.

|                   |                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | <b>no neighbor</b>                                                                                                                                                                                                                                                  |
| <b>Parameters</b> | <i>ip-address</i> — the neighbor IP address in dotted-decimal notation                                                                                                                                                                                              |
|                   | <b>Values</b> 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

|                    |                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>origin {igp   egp   incomplete   any}</b><br><b>no origin</b>                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry>from                                                                                                                                                                                                                                                 |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command removes the BGP origin attribute match criterion.                  |
| <b>Default</b>     | <b>no origin</b>                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <b>igp</b> — configures matching path information originating within the local AS<br><br><b>egp</b> — configures matching path information originating in another AS<br><br><b>incomplete</b> — configures matching path information learned by another method<br><br><b>any</b> — ignores this criteria |

## prefix-list

|                    |                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>prefix-list name [name...(up to 5 max)]</b><br><b>no prefix-list</b>                                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry>from<br>config>router>policy-options>policy-statement>entry>to                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures a prefix list as a match criterion for a route policy statement entry.<br><br>If no prefix list is specified, any network prefix is considered a match.<br><br>The prefix list specifies the network prefix (this includes the prefix and length) that a specific policy entry applies to.<br><br>Up to five prefix list names can be specified. |

## Route Policy Command Reference

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

|                    |                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>type</b> <i>type</i><br><b>no type</b>                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry>from                                                                                                                                                                                                          |
| <b>Description</b> | <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 <b>no</b> form of the command removes the OSPF type match criterion.</p> |
| <b>Parameters</b>  | <i>type</i> — the OSPF type metric                                                                                                                                                                                                                                |
| <b>Values</b>      | 1 — set as OSPF routes with type 1 LSAs<br>2 — set as OSPF routes with type 2 LSAs                                                                                                                                                                                |

---

## Route Policy Action Commands

### default-action

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-action {accept   next-entry   next-policy   reject}</b><br><b>no default-action</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>router>policy-options>policy-statement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command enables the context to configure actions for routes that do not match any route policy statement entries when the <b>accept</b> 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 <b>no</b> form of the command deletes the <b>default-action</b> context for the policy statement.</p> |
| <b>Default</b>     | <b>no default-action</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <p><b>accept</b> — routes matching the entry match criteria will be accepted and propagated</p> <p><b>next-entry</b> — 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><b>next-policy</b> — 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><b>reject</b> — routes matching the entry match criteria will be rejected</p>                                                                                                                                                                                                                                                     |

### action

|                    |                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>action {accept   next-entry   next-policy   reject}</b><br><b>no action</b>                                                                                                                           |
| <b>Context</b>     | config>router>policy-options>policy-statement>entry                                                                                                                                                      |
| <b>Description</b> | <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

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>as-path-prepend</b> <i>as-num</i> [ <i>repeat</i> ]<br><b>no as-path-prepend</b>                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <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 <b>no</b> form of the command disables the AS path prepend action from the route policy entry.</p> |
| <b>Default</b>     | <b>no as-path-prepend</b>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>as-num</i> — the AS number to prepend expressed as a decimal integer<br><b>Values</b> 1 to 4294967295<br><i>repeat</i> — the number of times to prepend the specified AS number expressed as a decimal integer<br><b>Values</b> 1 to 50                                                                                                                                                                                                       |

### community

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>community</b> {{ <b>add</b> <i>name</i> [ <b>remove</b> <i>name</i> ]}   { <b>remove</b> <i>name</i> [ <b>add</b> <i>name</i> ]}   { <b>replace</b> <i>name</i> }}<br><b>no community</b>                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <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 <b>add</b> and <b>remove</b> keywords.</p> <p>The <b>no</b> form of the command disables the action to edit the community path attribute for the route policy entry.</p> |
| <b>Default</b>     | <b>no community</b>                                                                                                                                                                                                                                                                                                                                                                                                                                        |

- 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
  - 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.

## damping

- Syntax** **damping** {*name* | **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** *name* — 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** *preference*  
**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** *preference* — the local preference expressed as a decimal integer
- Values** 0 to 4294967295

### metric

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>metric</b> { <b>add</b>   <b>subtract</b>   <b>set</b> } <i>metric</i><br><b>no metric</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | <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 <b>no</b> form of the command disables assigning a metric in the route policy entry.</p>                                                                                             |
| <b>Default</b>     | <b>no metric</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><b>add</b> — 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><b>subtract</b> — 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><b>set</b> — the specified metric replaces any existing metric</p> <p><i>metric</i> — the metric modifier expressed as a decimal integer</p> <p><b>Values</b>      0 to 4294967295</p> |

### next-hop

|                    |                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>next-hop</b> <i>ip-address</i><br><b>no next-hop</b>                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                                               |
| <b>Description</b> | <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 <b>no</b> form of the command disables assigning a next-hop address in the route policy entry.</p> |
| <b>Default</b>     | <b>no next-hop</b>                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <p><i>ip-address</i> — the next-hop IP address in dotted-decimal notation</p> <p><b>Values</b>      <i>ipv4-prefix:</i>                      a.b.c.d (host bits must be 0)<br/>                  <i>ipv4-prefix-length:</i>            0 to 32</p>                                                       |

## next-hop-self

|                    |                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] next-hop-self</b>                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                           |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command disables advertising the next-hop-self option for the route policy entry. |
| <b>Default</b>     | <b>no next-hop-self</b>                                                                                                                                                                                                                                                              |

## origin

|                    |                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>origin {igp   egp   incomplete}</b><br><b>no origin</b>                                                                                                                                                                                                           |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                           |
| <b>Description</b> | This command sets the BGP origin assigned to routes exported into BGP.<br><br>If the routes are exported into protocols other than BGP, this option is ignored.<br><br>The <b>no</b> form of the command disables setting the BGP origin for the route policy entry. |
| <b>Default</b>     | <b>no origin</b>                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <b>igp</b> — sets the path information as originating within the local AS<br><b>egp</b> — sets the path information as originating in another AS<br><b>incomplete</b> — sets the path information as learned by some other means                                     |

## preference

|                    |                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>preference <i>preference</i></b><br><b>no preference</b>                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                                                                                           |
| <b>Description</b> | This command assigns a route preference to routes matching the route policy statement entry.<br><br>If no preference is specified, the default route table manager (RTM) preference for the protocol is used.<br><br>The <b>no</b> form of the command disables setting an RTM preference in the route policy entry. |

## Route Policy Command Reference

|                   |                                                                         |
|-------------------|-------------------------------------------------------------------------|
| <b>Default</b>    | <b>no preference</b>                                                    |
| <b>Parameters</b> | <i>preference</i> — the route preference expressed as a decimal integer |
| <b>Values</b>     | 1 to 255 (0 represents unset, MIB only)                                 |

### tag

|                    |                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tag</b> <i>hex-string</i><br><b>no tag</b>                                                                                                                                                                                               |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                                  |
| <b>Description</b> | 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.<br><br>The <b>no</b> form of the command removes the tag. |
| <b>Default</b>     | <b>no tag</b>                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>hex-string</i> — assigns an OSPF tag                                                                                                                                                                                                     |
| <b>Values</b>      | OSPF: [0x0...0xFFFFFFFF]H                                                                                                                                                                                                                   |

### type

|                    |                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>type</b> <i>type</i><br><b>no type</b>                                                                                                                                                                                              |
| <b>Context</b>     | config>router>policy-options>policy-statement>default-action<br>config>router>policy-options>policy-statement>entry>action                                                                                                             |
| <b>Description</b> | 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 <b>no</b> form of the command disables assigning an OSPF type in the route policy entry. |
| <b>Default</b>     | <b>no type</b>                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>type</i> — specifies the OSPF type metric                                                                                                                                                                                           |
| <b>Values</b>      | 1 — set as OSPF routes with type 1 LSAs<br>2 — set as OSPF routes with type 2 LSAs                                                                                                                                                     |

---

## Show Commands

### policy

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>policy</b> [ <i>name</i>   <b>damping</b>   <b>prefix-list</b> <i>name</i>   <b>as-path</b> <i>name</i>   <b>community</b> <i>name</i>   <b>admin</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | show>router                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command displays configured policy statement information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <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><b>damping</b> — displays the damping profile for use in the route policy</p> <p><b>prefix-list</b> — displays the prefix lists configured in the route policy</p> <p><b>as-path</b> — displays AS path regular expression statements used in the route policy</p> <p><b>community</b> — displays community lists used in the route policy</p> <p><b>admin</b> — if this keyword is included, the entire policy option configuration is shown, including any uncommitted configuration changes. This command is similar to the <b>info</b> command.</p>                                                                                                                                                   |
| <b>Output</b>      | <p>The following outputs are examples of route policy information, and <a href="#">Table 27</a> describes the fields.</p> <ul style="list-style-type: none"><li>• <a href="#">Sample Output - show router policy</a></li><li>• <a href="#">Sample Output - show router policy admin</a></li><li>• <a href="#">Sample Output - show router policy name</a></li><li>• <a href="#">Sample Output - show router policy damping</a></li><li>• <a href="#">Sample Output - show router policy prefix-list</a></li><li>• <a href="#">Sample Output - show router policy prefix-list name</a></li><li>• <a href="#">Sample Output - show router policy as-path</a></li><li>• <a href="#">Sample Output - show router policy as-path name</a></li><li>• <a href="#">Sample Output - show router policy community</a></li><li>• <a href="#">Sample Output - show router policy community name</a></li></ul> |

### 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'"
```

```

 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 27: Show Route Policy Output Fields**

| <b>Label</b>   | <b>Description</b>                                                                                                                                                                                                        |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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<br>for Ethernet-based networks |

## Telecom Compliance

|                                      |                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| IC CS-03 Issue 9                     | Spectrum Management and<br>Telecommunications                                                                                             |
| ACTA TIA-968-A                       |                                                                                                                                           |
| AS/ACIF S016 (Australia/New Zealand) | Requirements for Customer<br>Equipment for connection to<br>hierarchical digital interfaces                                               |
| ITU-T G.703                          | Physical/electrical characteristics<br>of hierarchical digital interfaces                                                                 |
| ITU-T G.707                          | Network node interface for the<br>Synchronous Digital Hierarchy (SDH)                                                                     |
| ITU-T G.712-2001                     | Transmission performance<br>characteristics of pulse code<br>modulation channels                                                          |
| ITU-T G.957                          | Optical interfaces for equipments<br>and systems relating to the<br>synchronous digital hierarchy                                         |
| ITU-T V.24                           | List of definitions for interchange<br>circuits between data terminal<br>equipment (DTE) and data circuit-<br>terminating equipment (DCE) |
| ITU-T V.36                           | Modems for synchronous data<br>transmission using 60-108 kHz group<br>band circuits                                                       |

## Protocol Support

### ATM

|                              |                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| RFC 2514                     | Definitions of Textual Conventions and<br>OBJECT_IDENTITIES for ATM<br>Management, February 1999                                   |
| RFC 2515                     | Definition of Managed Objects for ATM<br>Management, February 1999                                                                 |
| RFC 2684                     | Multiprotocol Encapsulation over ATM<br>Adaptation Layer 5                                                                         |
| af-tm-0121.000               | Traffic Management Specification<br>Version 4.1, March 1999                                                                        |
| ITU-T Recommendation I.610   | B-ISDN Operation<br>and Maintenance Principles and Functions version<br>11/95                                                      |
| ITU-T Recommendation I.432.1 | B-ISDN user-<br>network interface - Physical layer specification:<br>General characteristics                                       |
| GR-1248-CORE                 | Generic Requirements for<br>Operations of ATM Network Elements (NEs). Issue<br>3 June 1996                                         |
| GR-1113-CORE                 | Bellcore, Asynchronous Transfer<br>Mode (ATM) and ATM Adaptation Layer (AAL)<br>Protocols Generic Requirements, Issue 1, July 1994 |
| AF-PHY-0086.001              | Inverse Multiplexing for ATM<br>(IMA)                                                                                              |

### BFD

|                                 |                                                                   |
|---------------------------------|-------------------------------------------------------------------|
| draft-ietf-bfd-mib-00.txt       | Bidirectional Forwarding<br>Detection Management Information Base |
| draft-ietf-bfd-base-o5.txt      | Bidirectional Forwarding<br>Detection                             |
| draft-ietf-bfd-v4v6-1hop-06.txt | BFD IPv4 and IPv6<br>(Single Hop)                                 |
| draft-ietf-bfd-multihop-06.txt  | BFD for Multi-hop<br>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 472 Graceful Restart Mechanism for BGP - GR Helper
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)

### **DHCP**

- RFC 1534 Interoperation between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)

### **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)

### **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-mppls-ldp-mib-07.txt  
 draft-ietf-ospf-mib-update-04.txt  
 draft-ietf-mppls-lsr-mib-06.txt  
 draft-ietf-mppls-te-mib-04.txt  
 IANA-IFTtype-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

### 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+

- draft-grant-tacacs-02.txt The TACACS+ Protocol

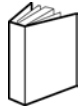
### TCP/IP

- 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

### 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://www.alcatel-lucent.com/support>



## Documentation feedback

[documentation.feedback@alcatel-lucent.com](mailto:documentation.feedback@alcatel-lucent.com)

