Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 1.1

ROUTER CONFIGURATION GUIDE

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

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

List of Tables

List of Figures

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
ABR	available bit rate
AC	alternating current attachment circuit
ACL	access control list
ACR	adaptive clock recovery
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
ARP	address resolution protocol
AS	autonomous system
ASAP	any service, any port
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
B-bit	beginning bit (first packet of a fragment)
Batt A	battery A
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BITS	building integrated timing supply
BOF	boot options file

Acronym	Expansion
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
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
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
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)
CSM	Control and Switching Module
CSPF	constrained shortest path first

Acronym	Expansion
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DDoS	distributed DoS
DHCP	dynamic host configuration protocol
DNS	domain name server
DoS	denial of service
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
e911	enhanced 911 service
E-bit	ending bit (last packet of a fragment)
ECMP	equal cost multi-path
EFM	Ethernet in the first mile
ELER	egress label edge router
Epipe	Ethernet VLL
ESD	electrostatic discharge
ETE	end-to-end

Acronym	Expansion
EVDO	evolution - data optimized
EXP bits	experimental bits
FC	forwarding class
FCS	frame check sequence
FDB	forwarding database
FDL	facilities data link
FEC	forwarding equivalence class
FIB	forwarding information base
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HEC	header error control
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
IBN	isolated bonding networks
ICMP	Internet control message protocol
ICP	IMA control protocol cells
IEEE	Institute of Electrical and Electronics Engineers
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module

Acronym	Expansion
IP	Internet Protocol
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LLID	loopback location ID
LSP	label switched path
LSR	label switch router
LTN	LSP ID to NHLFE
MAC	media access control
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MD5	message digest version 5 algorithm
MDA	media dependent adapter
MEF	Metro Ethernet Forum
MFC	multi-field classification
MIB	management information base
MIR	minimum information rate
MLPPP	multilink point-to-point protocol
MP	multilink protocol
MPLS	multiprotocol label switching
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit

Acronym	Expansion
NHLFE	next hop label forwarding entry
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)
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OS	operating system
OSS	operations support system
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
POP	point of presence
PPP	point-to-point protocol
PSN	packet switched network
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE3	pseudowire emulation edge-to-edge
QoS	quality of service
RAN	Radio Access Network
RDI	remote defect indication

Acronym	Expansion
RED	random early discard
RNC	Radio Network Controller
RSVP-TE	resource reservation protocol - traffic engineering
R&TTE	Radio and Telecommunications Terminal Equipment
RT	receive/transmit
RTM	route table manager
RTN	battery return
RTP	real-time protocol
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
SDP	service destination point
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	simple network time protocol
SPE	source provider edge router
SPF	shortest path first
SR	service router (includes 7710 SR, 7750 SR)
SSH	secure shell
SSU	system synchronization unit
SVC	switched virtual circuit
TCP	transmission control protocol
TDM	time division multiplexing

Acronym	Expansion
TLDP	targeted LDP
TLV	type length value
ToS	type of service
TPE	target provider edge router
TPID	tag protocol identifier
TTL	time to live
TTM	tunnel table manager
UBR	unspecified bit rate
UDP	user datagram protocol
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPN	virtual private network
VPRN	virtual private routed network
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard

Preface

About This Guide

This guide describes logical IP routing interfaces, IP-based filtering, and routing policy support provided by the Alcatel-Lucent 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) 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, user services, and Operations, Administration and Management (OAM) tools.
- 7705 SAR OS Quality of Service Guide

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

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

Getting Started

In This Chapter

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

7705 Service Aggregation 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 25
Protocol configuration	Configure IP filters	Filter Policies on page 93
	Configure routing policies	Route Policies on page 141
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 179

Notes on 7705 SAR-8 and 7705 SAR-F

The 7705 SAR-F and the 7705 SAR-8 run the same operating system software. The main difference between the products is their hardware configuration. The 7705 SAR-8 has an 8-slot chassis that supports two CSMs, six adapter cards, and a Fan module. The 7705 SAR-F chassis has a fixed hardware configuration, replacing the 7705 SAR-8 physical components (the CSM, Fan module, and adapter cards) 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 a 16-port T1/E1 ASAP Adapter card on the 7705 SAR-8 with additional support for multiple synchronization sources. The 7705 SAR-8 CLI indicates that the MDA type for the T1/E1 ASAP Adapter card is `a16-chds1`. The 7705 SAR-F supports MDA type `a16-chds1v2`.
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	The Ethernet ports on the 7705 SAR-F are equivalent to one 8-port Ethernet Adapter card (version 2) on the 7705 SAR-8 with additional support for multiple synchronization sources. The 7705 SAR-8 CLI indicates that the MDA type for the Ethernet Adapter card is `a8-eth` or `a8-ethv2`. The 7705 SAR-F supports MDA type `a8-ethv3`. Versions 2 and 3 support Synchronous Ethernet timing.

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

7705 SAR-8	7705 SAR-F	Notes
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

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. Once 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, unless overwritten by an explicit router ID. In Release 1.1, the router ID is not configurable and is always the system interface. Future releases will allow overwriting or configuration of the router ID.

The following router parameters can be configured:

- Interfaces
- IP Addresses
- Static Routes and ECMP

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 is restricted to control plane messaging (including MPLS signaling, next-hop address resolution, management traffic (SNMP), and for OAM purposes). In Release 1.1 static routes to next-hop addresses are supported. No dynamic routing protocols are supported in this release.

Ethernet Ports and Associated MAC Addresses

When an Ethernet port is configured with an IP address, a MAC address is automatically associated with the port. In Release 1.1 of the 7705 SAR, only one MAC address can be associated with an Ethernet port on the Ethernet Adapter card. However, it is possible to change the default MAC address at the port level. For information on changing the MAC address associated with an Ethernet port, see the 7705 SAR OS Interface Configuration Guide.

Dynamic ARP and Static MAC entry

In Release 1.1, only one MAC address per IP interface can be learned. The MAC address of the far end can be learned dynamically or be statically configured.

ARP is the common way to resolve the MAC address of next-hop IP hosts and is the primary way to resolve IP-to-MAC associations in Release 1.1. 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 in Release 1.1. 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 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.

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 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.

Static Routes and ECMP

In Release 1.1, only static routes to next-hop addresses are supported. No dynamic routing protocols are supported in this release.

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.

There can be multiple parallel links between the 7705 SAR and an upstream peer; therefore, ECMP can be enabled to distribute the MPLS traffic across the links in order to balance the traffic load. 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.

Since IP routing is used exclusively for control plane messaging (for example, MPLS signaling), the IP packets are not load-balanced; rather, ECMP is used to load balance pseudowire traffic. Load distribution is done on a per-service basis.

In the receive direction, the 7705 SAR does support extraction and processing of load-balanced IP and VLL traffic sent from other routers.

Bidirectional forwarding detection (BFD) for static routes

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. In Release 1.1 of the 7705 SAR, 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.

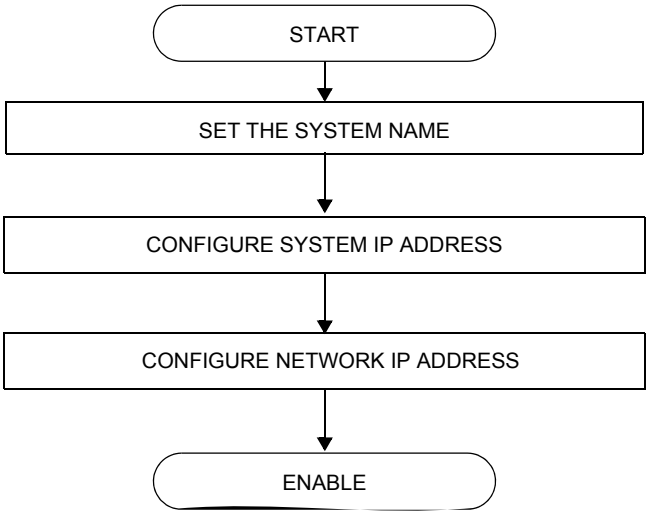
Due to the lightweight nature of BFD, it can detect failures faster than other detection protocols, making it ideal for use in applications such as mobile transport.

If the configured number of BFD messages is not received in the configured timeframe, the static route to the peer is declared not active.

Router Configuration Process Overview

Figure 1 displays the process to configure basic router parameters.

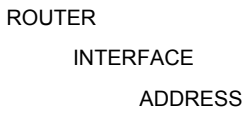
Figure 1: IP Router Configuration Flow



Router Configuration Components

Figure 2 displays the basic router configuration components.

Figure 2: Router Configuration Components



The basic router parameters in Figure 2 are described as follows:

- Interface — a logical IP routing interface. Once created, attributes like an IP address, port, or the system can be associated with the IP interface. The system interface is the loopback address and is also the router ID. It is associated with the network entity. The network interface is associated with a logical or physical port.
- Address — the address associates the device's system name with the IP system address. An IP address must be assigned to each IP interface. Only IPv4 addresses are supported in Release 1.1 of the 7705 SAR.

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 179.

Configuring an IP Router with CLI

This section provides information to configure an IP router.

Topics in this section include:

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. This is the global router configuration context where objects like static routes 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 static routes

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 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 reestablished over the alternate routes. The system interface IP address is also used for pseudowire/VLL signaling (via targeted LDP).

The system interface has an implied router identifier that is not user-configurable (as it is on products such as the 7710 SR and 7750 SR) and is not something a user would see. The router ID is used implicitly for some operations; for example, ICMP messaging uses the router ID. In Release 1.1, the router ID is the same as the system IP interface.

Network Interface

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

CLI Command Structure

Figure 3 displays the basic CLI command structure to configure router parameters. The commands are located under the `config>router` context.

Figure 3: CLI Configuration Context

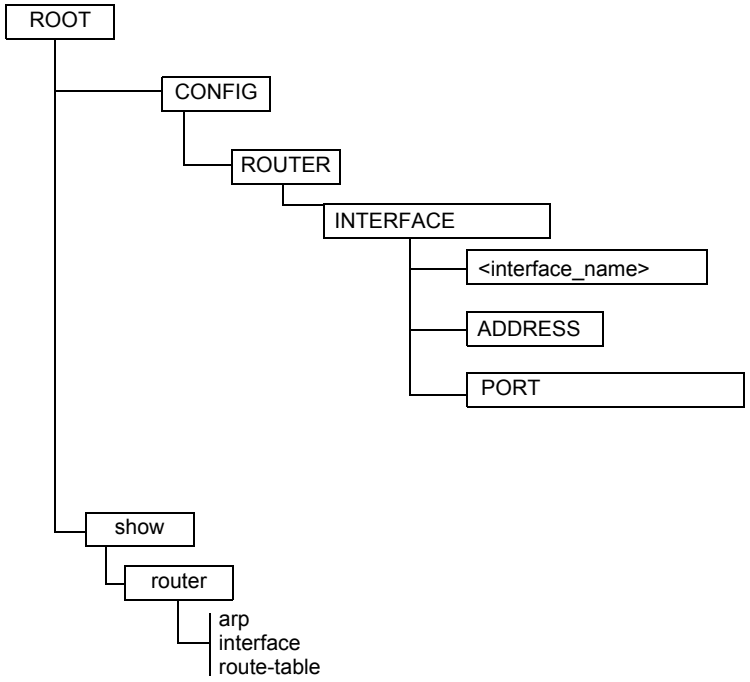
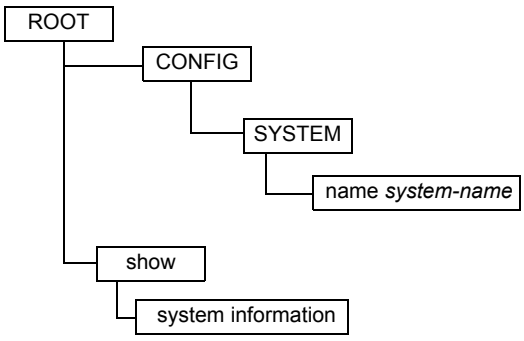


Figure 4 displays the brief CLI command structure to configure the system name. The commands are located under the `config>system` context.

Figure 4: CLI System Configuration Context



See the 7705 SAR OS Basic System Configuration Guide for more information on system command syntax and descriptions

List of Commands

Table 3 lists all the configuration commands to configure a 7705 SAR router, indicating the configuration level at which each command is implemented with a short command description.

The command list is organized in the following task-oriented manner:

- Configure the system name
- Configure router parameters
- Configure a network interface
- Configure the system interface
- Configure interface ICMP

Table 3: CLI Commands to Configure Basic IP Router Parameters

Command	Description	Page
Configure the system name		
`config>system`		
`name`	The system name for the device. Only one system name can be configured.	41
Configure router parameters		
`config>router`		41
`ecmp`	Enables ECMP and configures the number of routes for path sharing	55
`interface`	Creates, deletes, or configures a logical IP interface	58
`ldp`	Refer to the 7705 SAR OS MPLS Guide for configuration information	–
`mpls`	Refer to the 7705 SAR OS MPLS Guide for configuration information	–
`policy-options`	Refer to Route Policies for configuration information	141
`static-route`	Creates or deletes static route entries	56
Configure a network interface		
`config>router>interface`		42
`address`	Assigns an IP address and subnet mask to an IP interface. Only one IP address is associated with an IP interface.	59

Table 3: CLI Commands to Configure Basic IP Router Parameters (Continued)

Command	Description	Page
`arp-timeout`	Configures the minimum time in seconds that an address resolution protocol (ARP) entry learned on the IP interface will be stored in the ARP table	60
`bfd`	Configures the minimum transmit and receive intervals that a specified number of control messages should be sent and received before a network failure is declared	61
`description`	Adds an ASCII string describing the interface to the configuration file	54
`icmp`	Configures ICMP parameters for the interface	65
`ingress`	Configures ingress network filter policies for the interface	64
`ntp-broadcast`	Enables or disables receiving of SNTP broadcasts on the IP interface	61
`port`	Creates an association between an IP interface and a physical port	62
`qos`	Associates a network Quality of Service (QoS) policy with an IP interface	62
`shutdown`	Administratively enables or disables the interface	54
`static-arp`	Configures a static ARP entry associating an IP address with a MAC address for the interface	63
Configure the system interface		
`config>router>interface`		42
`address`	Assigns an IP address and IP subnet mask to an IP interface. Only one IP address can be associated with an IP interface.	59
`description`	Adds an ASCII string describing the interface to the configuration file	54
`shutdown`	Administratively enables or disables the interface	54
Configure interface ICMP		
`config>router>interface`		
`icmp`	Configures ICMP parameters on a network IP interface	65
`mask-reply`	Enables responses to ICMP mask requests on the router interface	65
`ttl-expired`	Configures the rate that ICMP TTL expired messages are issued by the interface	65
`unreachables`	Enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface	66

Basic Configuration

Note: Refer to Filter Policies on page 93 and Route Policies on page 141 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 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 in 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
-------------------------------------------------
A#ALU-A>config>system#
```

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.

Note that 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 is used to distribute the MPLS traffic across the links to balance the traffic load. Since IP routing is used exclusively for control plane messaging (for example, MPLS signaling), the IP packets are not load-balanced; rather, ECMP is used to load balance pseudowire traffic. Load distribution is done per service, not per packet.

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

In Release 1.1 of the 7705 SAR, only static routes to next-hop addresses are supported. No dynamic routing protocols are supported in this release. Black-hole routing is also not supported in this release.

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} [metric metric] [enable |
        disable] next-hop
        {ip-in-name | ip-address} [bfd-enable]
```

Example:
```
config>router# static-route 192.168.250.0/24 metric 1
  enable next-hop 10.200.10.3
config>router# exit
```

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

Deleting a Logical IP Interface

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

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

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

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

IP Router Command Reference

Command Hierarchies

Configuration Commands

Router Commands

```
config
    — router [router-name]
        — ecmp max-ecmp-routes
        — no ecmp
        — [no] interface ip-int-name
        — [no] ldp
        — [no] mpls
        — [no] policy-options
        — [no] interface {ip-prefix/prefix-length | ip-prefix netmask} [metric metric]
          [enable | disable] next-hop {ip-int-name | ip-address} [bfd-enable]
```

Router Interface Commands

```
config
    — router [router-name]
        — [no] interface ip-int-name
            — address {ip-address/mask | ip-address netmask}
            — no address
            — arp-timeout seconds
            — no arp-timeout
            — bfd transmit-interval [receive receive-interval] [multiplier multiplier]
            — no bfd
            — description description-string
            — no description
            — 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]
            — ntp-broadcast seconds
            — no ntp-broadcast
            — port port-name
            — no port
            — qos network-policy-id
            — no qos
            — [no] shutdown
            — static-arp ip-addr ieee-mac-addr
            — nostatic-arp ip-addr
```

Show Commands

```
show
    — router router-instance
        — arp [ip-int-name | ip-address/[mask] | mac ieee-mac-address | summary] [local | dynamic |
          static | managed]
        — authentication
            — statistics
            — statistics interface [ip-int-name | ip-address]
            — statistics policy name
        — bfd
            — interface
            — session [src ip-address [dst ip-address] | [detail]]
        — ecmp
        — fib slot-number [family] [ip-prefix/prefix-length] [longer]
        — interface [{[ip-address | ip-int-name] [detail]} | [summary] | [exclude-services]
        — interface family [detail]
        — ldp
        — mpls
        — policy
        — route-table [ip-prefix[/prefix-length] [longer | exact]] | [protocol protocol-name] |
          [summary]
        — static-arp [ip-address | ip-int-name | mac ieee-mac-addr]
        — static-route [family] [[ip-prefix[/mask]] | [preference preference] | [next-hop ip-address]|
          [tag tag]
        — 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
        — interface [ip-int-name | ip-addr] [icmp]
        — ldp
        — mpls
```

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**] **ip**
    - [no] **arp**
    - **icmp**
    - **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**] **ldp**
  - [**no**] **mpls**

Note: For information on MPLS and LDP, see the 7705 SAR OS MPLS Guide. For information on policy options, see Route Policies on page 141.

Configuration Commands

Generic Commands

description

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

Context config>router>interface *ip-int-name*

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 is associated with the configuration context.

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

shutdown

Syntax **shutdown**
no shutdown

Context config>router>interface *ip-int-name*

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** *router-name*

Context config

Description This command enables the context to configure router parameters, interfaces, route policies, and protocols.

Parameters *router-name* — the router name

Values router-name: Base, management

Default Base

ecmp

Syntax **ecmp** *max-ecmp-routes*
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 is used to distribute MPLS traffic across the links to balance the traffic load. Since IP routing is restricted to MPLS signaling, the IP packets are not load-balanced; rather, ECMP is used to load balance pseudowire traffic for VLL services. Distribution is done per service, not per packet.

All valid LDP next-hop peers (that is, those peers that sent a label mapping for a given IP prefix) are installed in the forwarding plane. As an ingress LER, the 7705 SAR maps an ingress label to all the next-hops. The forwarding plane then uses an internal hashing algorithm to determine how the traffic will be distributed amongst the multiple next-hops.

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

Default **no ecmp**

Parameters *max-ecmp-routes* — the maximum number of equal cost routes allowed on this routing table instance, expressed as a decimal integer. Setting ECMP *max-ecmp-routes* to 1 yields the same result as entering **no ecmp**.

Values 0 to 8

static-route

Syntax [**no**] **static-route {*ip-prefix/prefix-length* | *ip-prefix netmask*}** [**metric *metric***] [**enable | disable**] **next-hop {*ip-int-name* | *ip-address*}** [**bfd-enable**]

Context config>router

Description This command creates static route entries for network routes. When configuring a static route, the **next-hop** 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, then as many parameters to uniquely identify the static route must be entered.

Default No static routes are defined.

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)

metric *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. When the metric is configured as 0, then the metric configured in OSPF, default-import-metric, 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, then the lower-cost (metric) route will be installed.
- If there are multiple static routes with equal metrics, then ECMP rules apply.

Default 1

Values 0 to 65535

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

next-hop [*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

Router Interface Commands

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router

Description This command creates a logical IP routing interface. Once created, attributes like IP address, port, or system can be associated with the IP interface.

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.

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.

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.

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.

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.

Default No interfaces or names are defined within the system.

Parameters *ip-int-name* — 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.

Values 1 to 32 alphanumeric characters (must start with a letter)

If the *ip-int-name* already exists, the context is changed to maintain that IP interface. If the *ip-int-name* 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 *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

address

Syntax **address** {*ip-address*/*mask* | *ip-address netmask*}
no address

Context config>router>interface *ip-int-name*

Description This command assigns an IP address and IP subnet to an IP interface. Only one IP address can be associated with an IP interface.

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.

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.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

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.

To change an IP address, perform the following steps:

1. Shut down the router interface.
2. Assign the new IP address.
3. Enable the router interface.

If a new address is entered while another address is still active, the new address will be rejected.

Default No IP address is assigned to the IP interface.

Parameters *ip-address* — the IP address of the IP interface. The *ip-address* 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.

Values 1.0.0.0 to 223.255.255.255

/ — the forward slash is a parameter delimiter that separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "/" and the *mask* parameter. If a forward slash does not immediately follow the *ip-address*, a dotted decimal mask must follow the prefix.

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)

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context config>router>interface *ip-int-name*

Description This command configures the minimum time, 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 seconds, ARP aging is disabled.

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

Note: ARP entries will refresh 30 s before they expire, but only if the ARP timeout is set to more than 45 s.

Default **no arp-timeout**

Parameters *seconds* — 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 seconds (4 hours)

bfd

Syntax **bfd** {*transmit-interval*} [**receive** *receive-interval*] [**multiplier** *multiplier*]
no bfd

Context config>router>interface *ip-int-name*

Description This command configures the time interval in which BFD control messages are transmitted and received on the interface and the number of control messages to be transmitted and received within that interval. This mechanism is used to detect failures in the network. If either end does not receive the specified number of messages in the specified time interval, the far end is declared to be down.

Default **no bfd**

Parameters *transmit-interval* — the number of milliseconds between transmitted control messages

Values 100 to 100000

Default 100

receive-interval — the number of millseconds between received control messages

Values 100 to 100000

Default 100

multiplier — the number of control messages to be sent during the configured transmit and receive intervals

Values 3 to 20

Default 3

ntp-broadcast

Syntax **ntp-broadcast**
no ntp-broadcast

Context config>router>interface *ip-int-name*

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** *port-name*
no port

Context config>router>interface *ip-int-name*

Description This command creates an association with a logical IP interface and a physical port.

An interface can also be associated with the system (loopback address).

The command returns an error if the interface is already associated with another port or the system. In this case, the association must be deleted before the command is reattempted.

The port name consists of the *port-id* (for T1/E1 interfaces and Ethernet interfaces) and an optional encapsulation value (for Ethernet interfaces). The port name can also be the *bundle-id* used for the multilink bundle associated with the interface. See the 7705 SAR OS Interface Configuration Guide for information on configuring ports.

The **no** form of the command deletes the association with the port. The **no** form of this command can only be performed when the interface is administratively down.

Default No port is associated with the IP interface.

Parameters *port-name* — the physical port identifier to associate with the IP interface

Values

port-id	*slot/mda/port*	
bundle-id	*bundle-type-slot/mda.bundle-num*	
	bundle	keyword
	type	ima, ppp
	bundle-num	1 to 128
encap-val	0 (for null) 0 to 4094 (for dot1q)	

qos

Syntax **qos** *network-policy-id*
no qos

Context config>router>interface *ip-int-name*

Description This command associates a network Quality of Service (QoS) policy with an IP interface.

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.

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.

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 *network-policy-id* — 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** *ip-addr ieee-mac-addr*
no static-arp *ip-addr*

Context config>router>interface

Description 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.

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.

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.

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. Thus, 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.

The **no** form of the command removes a static ARP entry.

Default No static ARPs are defined.

Parameters *ip-addr* — the IP address for the static ARP in IP address dotted decimal notation

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

Router Interface Filter Commands

ingress

Syntax **ingress**

Context config>router>interface *ip-int-name*

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** *ip-filter-id*
no filter
no filter [**ip** *ip-filter-id*]

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 *ip-filter-id* must have been pre-configured 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 **ip** *ip-filter-id* — 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 108.

Router Interface ICMP Commands

icmp

Syntax **icmp**

Context config>router>interface *ip-int-name*

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 **mask-reply**
no mask-replay

Context config>router>if>icmp

Description This command enables or disables responses to ICMP mask requests on the router interface.

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.

The **no** form of the command disables replies to ICMP mask requests on the router interface.

Default **mask-reply —** replies to ICMP mask requests

ttl-expired

Syntax **ttl-expired** [*number seconds*]
no ttl-expired

Context config>router>if>icmp

Description This command configures the rate that ICMP Time To Live (TTL) expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10-second time interval.

The **no** form of the command disables the generation of TTL expired messages.

Default **ttl-expired 100 10** — maximum of 100 TTL expired message in 10 seconds

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 1000

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 unreachables

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-second 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 seconds

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 1000

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.

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

mac *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

Output **ARP Table Output —** The following table describes the ARP table output fields.

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	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

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#
```

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 **interface** [*ip-int-name* | *ip-address*] — specifies an existing interface name or IP address

Values

ip-int-name	32 chars max
ip-address	a.b.c.d

policy *name* — specifies an existing policy name

Output **Authentication Statistics Output —** The following table describes the authentication statistics output fields.

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

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#
```

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 **BFD interface Output —** The following table describes the BFD interface output fields.

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.

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
===============================================================================
```

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 **BFD Session Output —** The following table describes the BFD session output fields.

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

Sample Output

```
*A:ALU-1# show router bfd session
===============================================================================
BFD Session
===============================================================================
Interface                     State                   Tx Intvl  Rx Intvl  Mult
  Remote Address              Protocol                Tx Pkts   Rx Pkts
-------------------------------------------------------------------------------
net1_1_2                      Up (3)                  100       100       3
   12.1.2.1                   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#
```

ecmp

Syntax **ecmp**

Context show>router

Description This command displays the ECMP settings for the router.

Output **ECMP Settings Output —** The following table describes the output fields for the router ECMP settings.

Table 8: 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

Sample Output

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

fib

Syntax **fib** *slot-number* [*family*] [*ip-prefix/prefix-length*] [**longer**]

Context show>router

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

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

Values 1

family — displays the specified router IP interface table

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

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

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 **Standard IP Interface Output —** The following table describes the standard output fields for an IP interface.

Table 9: 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

Table 9: Show Standard IP Interface Output Fields (Continued)

Label	Description
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

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

Detailed IP Interface Output — The following table describes the detailed output fields for an IP interface.

Table 10: 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
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	For Release 1.1, 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 1.1, 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
Arp Timeout	The ARP timeout for the interface, in seconds, which is the time 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

Table 10: Show Detailed IP Interface Output Fields (Continued)

Label	Description
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-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    : None
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#
```

Summary IP Interface Output — The following table describes the summary output fields for the router IP interfaces.

Table 11: 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

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#
```

route-table

Syntax **route-table** [**family**] [*ip-prefix*[/*prefix-length*] [**longer** | **exact**]] | [**protocol** *protocol-name*] | [**summary**]

Context show>router

Description This command displays the active routes in the routing table.

If no command line arguments are specified, all routes are displayed, sorted by prefix.

Parameters **family** — specifies the type of routing information to be distributed by this peer group

Values **ipv4** — displays only those BGP peers that have the IPv4 family enabled and not those capable of exchanging IP-VPN routes

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-legnth* and routes with longer masks

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

protocol *protocol-name* — displays routes learned from the specified protocol

Values static

summary — displays route table summary information

Output **Standard Route Table Output —** The following table describes the standard output fields for the route table.

Table 12: 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

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#
```

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.

Parameters *ip-address* — only displays the static ARP entry associated with the specified IP address

ip-int-name — only displays the static ARP entry associated with the specified IP interface name

mac *ieee-mac-addr* — only displays the static ARP entry associated with the specified MAC address

Output **Static ARP Table Output —** The following table describes the output fields for the ARP table.

Table 13: 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

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#
```

static-route

Syntax **static-route** [**family**] [[*ip-prefix* [*/mask*]] | [**preference** *preference*] | [**next-hop** *ip-address*] | **tag** *tag*]

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 **family** — specifies the type of routing information to be distributed by this peer group

Values **ipv4** — displays only those BGP peers that have the IPv4 family enabled and not those capable of exchanging IP-VPN routes

ip-prefix[*/mask*] — displays static routes only matching the specified *ip-prefix* and optional *mask*

Values

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

preference *preference* — only displays static routes with the specified route preference

Values 0 to 65535

next-hop *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 *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

Output **Static Route Output —** The following table describes the output fields for the static route table.

Table 14: Show Static Route Table Output Fields

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

Table 14: Show Static Route Table Output Fields (Continued)

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

Sample Output

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

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

status

Syntax **status**

Context show>router

Description This command displays the router status.

Output **Router Status Output —** The following table describes the output fields for router status information.

Table 15: Show Router Status Output Fields

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

Sample Output

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

===============================================================
Router Status (Router: Base)
===============================================================
                         Admin State         Oper State
---------------------------------------------------------------
Router                   Up                  Up
MPLS                     Up                  Down
LDP                      Up                  Down

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

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 **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 *protocol* — displays LDP protocol information

sdp *sdp-id* — displays information pertaining to the specified SDP

summary — displays summary tunnel table information

Output **Tunnel Table Output —** The following table describes tunnel table output fields.

Table 16: 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

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# show router tunnel-table summary
===============================================================================
Tunnel Table Summary (Router: Base)
===============================================================================
                              Active                   Available
-------------------------------------------------------------------------------
LDP                           1                        1
SDP                           1                        1
===============================================================================
*A:ALU-1#
```

Clear Commands

arp

Syntax **arp** {**all** | *ip-addr* | **interface** {*ip-int-name* **|** *ip-addr*}}

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

ip-addr — clears the ARP cache entry for the specified IP address

interface *ip-int-name* **—** clears all ARP cache entries for the IP interface with the specified name

interface *ip-addr* **—** clears all ARP cache entries for the specified IP interface with the specified IP address

authentication

Syntax **authentication statistics** [**interface** {*ip-int-name* | *ip-address*}]

Context clear>router

Description This command clears router authentication statistics.

Parameters *ip-int-name* — clears the statistics for the specified interface name

Values 32 characters maximum

ip-address — 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** *ip-address* **dst-ip** *ip-address*
session all

Context clear>router>bfd

Description This command clears BFD sessions.

Parameters **src-ip** *ip-address* **—** specifies the address of the local endpoint of this BFD session

dst-ip *ip-address* **—** specifies the address of the far-end endpoint of this BFD session

all — clears all BFD sessions

statistics

Syntax **statistics src-ip** *ip-address* **dst-ip** *ip-address*
statistics all

Context clear>router>bfd

Description This command clears BFD statistics.

Parameters **src-ip** *ip-address* **—** specifies the address of the local endpoint of this BFD session

dst-ip *ip-address* **—** specifies the address of the remote endpoint of this BFD session

all — clears statistics for all BFD sessions

interface

Syntax **interface** [*ip-int-name* | *ip-addr*] [**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** *trace-destination*

Context debug>trace

Description This command specifies the destination to send trace messages.

Parameters *trace-destination* — the destination to send trace messages to

Values stdout, console, logger, memory

enable

Syntax **enable**
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** ***module-name***] [**type** ***event-type***] [**class** ***event*-class**] [**task** ***task-name***] [**function** ***function-name***]

Context debug>trace

Description This command adds trace points.

The **no** form of the command removes the trace points.

router

Syntax **router** *router-instance*

Context debug

Description This command configures debugging for a router instance.

Parameters **router-instance —** The router name or service ID.

Values *router-name* Base, management
service-id 1 to 2147483647

Default Base

ip

Syntax **ip**
no ip

Context debug>router

Description This command configures debugging for IP.

arp

Syntax **arp**
no arp

Context debug>router>ip

Description This command enables or disables ARP debugging.

icmp

Syntax **icmp**
no icmp

Context **debug>router>ip**

Description This command enables or disables ICMP debugging.

interface

Syntax [**no**] **interface** [*ip-int-name* | *ip-address*]

Context debug>router>ip

Description This command enables or disables debugging for virtual interfaces.

Parameters *ip-int-name* — only displays the interface information associated with the specified IP interface

Values 32 characters maximum

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)

neighbor

Syntax **neighbor**
no neighbor

Context debug>router>ip

Description This command enables or disables neighbor debugging.

packet

Syntax **packet** [*ip-int-name* | *ip-address*] [**headers**] [*protocol-id*]
no packet [*ip-int-name* | *ip-address*]

Context debug>router>ip

Description This command enables or disables debugging for IP packets.

Parameters *ip-int-name* — only displays the interface information associated with the specified IP interface

Values 32 characters maximum

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

Values a.b.c.d

headers — only displays information associated with the packet header

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

Values 0 to 255 (values can be expressed in decimal, hexidecimal, or binary)
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

route-table

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

Context debug>router>ip

Description This command configures route table debugging.

Parameters *ip-prefix/prefix-length* — the IP prefix for prefix list entry in dotted decimal notation

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

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

Filter Policies

In This Chapter

This chapter provides information about filter policies and management.

Topics in this chapter include:

Configuring Filter Policies

Filter policies, also referred to as Access Control Lists (ACLs), are templates applied to ports to control ingress network traffic based on IP matching criteria.

In Release 1.1 of the 7705 SAR, filters are applied to ingress network ports only. Ingress filters affect only inbound traffic destined for the control plane. Basic IP filters are implemented mainly to protect the control plane from distributed DoS attacks, unauthorized access, and similar security breaches. As well, the IP filters are used to limit management access to the 7705 SAR. Filters can be used to limit which interface can be used for management traffic or to restrict the IP range that can access the 7705 SAR for management purposes.

Configuring an entity with a filter policy is optional. If a network port is not configured with filter policies, then all traffic is allowed on the ingress interfaces. By default, there are no filters associated with interfaces. The filters must be explicitly created and associated. When you create a new filter, default values are provided although you must specify a unique filter ID value to each new filter policy as well as each new filter entry and associated actions. The filter entries specify the filter matching criteria.

Network Port-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 8 IP filter policies per node. Within each filter policy, you can create up to 30 entries.

Filter entry matching criteria can be as general or specific as you require, 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.

Filter Policy Entities

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

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

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

Each filter entry contains:

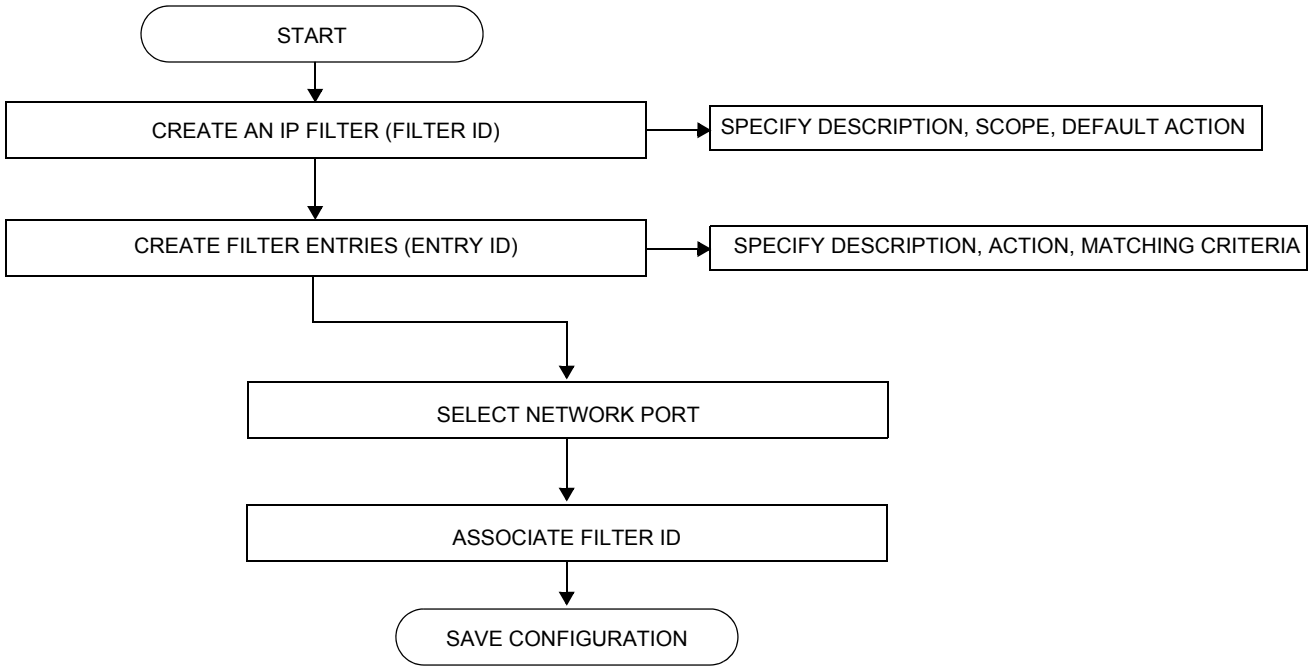
- match criteria
- an action

Applying Filter Policies

Filter policies can be applied to network ingress IP interfaces.

Figure 5 displays the process to create filter policies and apply them to a network port.

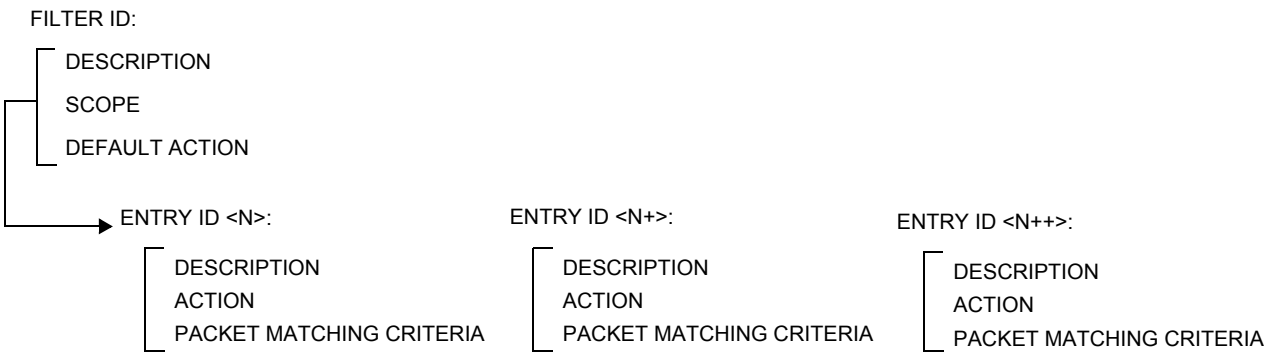
Figure 5: Creating and Applying Filter Policies



Policy Components

Figure 6 displays the major components of a filter policy.

Figure 6: Filter Policy Components



- Filter ID (mandatory) — the value that identifies the filter
- Description (optional) — provides a brief overview of the filter's features
- Scope (mandatory) — a filter policy must be defined as having either an *exclusive* scope for one-time use, or a *template* scope that enables its use with multiple interfaces
- Default action (mandatory) — specifies the action to be applied to packets when no action is specified in the IP filter entries or when the packets do not match the specified criteria. The default action is always Drop.
- Entry ID (one or more) — Each entry represents a collection of filter match criteria. Packet matching begins the comparison process with the criteria specified in the lowest entry ID.

Entries identify attributes that define matching conditions and actions. All criteria in the entry must match in order for the specified action to be taken. Each entry consists of the following components:

- → Entry ID (mandatory) — determines the order amongst all entry IDs, within a specific filter ID, in which the matching criteria specified in the collection is compared. Packets are compared to entry IDs in ascending order.
- → Description (optional) — the description should provide a brief overview of the entry ID criteria
- → Action (mandatory) — 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.
- → Packet matching criteria — you can input and select criteria to create a specific template through which packets are compared and either forwarded or dropped, depending on the action specified

Packet Matching Criteria

Up to 8 IP filter IDs (unique filter policies) can be defined. The ID can be a value from 1 to 65535. A maximum of 30 filter entries can be defined in one filter at the same time.

For filter entries 1 to 29, the match parameters can be any combination of source IP address/range, destination IP address/range, source port/range, and destination port/range as long as the accumulated total of the number of unique records does not exceed 256 entities. For example, an entry with /29 would count as 8 entities. For filter entry 30, there are no range-based restrictions. As few or as many match parameters can be specified as required.

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.

IP filter policies match criteria that associate traffic with an ingress 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).
- source IP address and mask — source IP address and mask values can be entered as search criteria. The IP Version 4 addressing scheme consists of 32 bits expressed in dotted decimal notation (X.X.X.X).

  Address ranges are configured by specifying mask values, the 32-bit combination used to describe the address portion that refers to the subnet and which portion refers to the host. The mask length is expressed as an integer (range 1 to 32).
- destination IP address and mask — destination IP address and mask values can be entered as search criteria
- source port/range — entering the source port number or port range allows the filter to search for matching TCP or UDP port and range values
- destination port/range — entering the destination port number or port range allows the filter to search for matching TCP or UDP values
- ICMP code — entering an ICMP code allows the filter to search for matching ICMP code in the ICMP header
- ICMP type — entering an ICMP type allows the filter to search for matching ICMP types in the ICMP header

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, edit the entry ID value; for example, to reposition entry ID 6 to a more explicit location, change the entry ID *6* value to entry ID *2*.

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

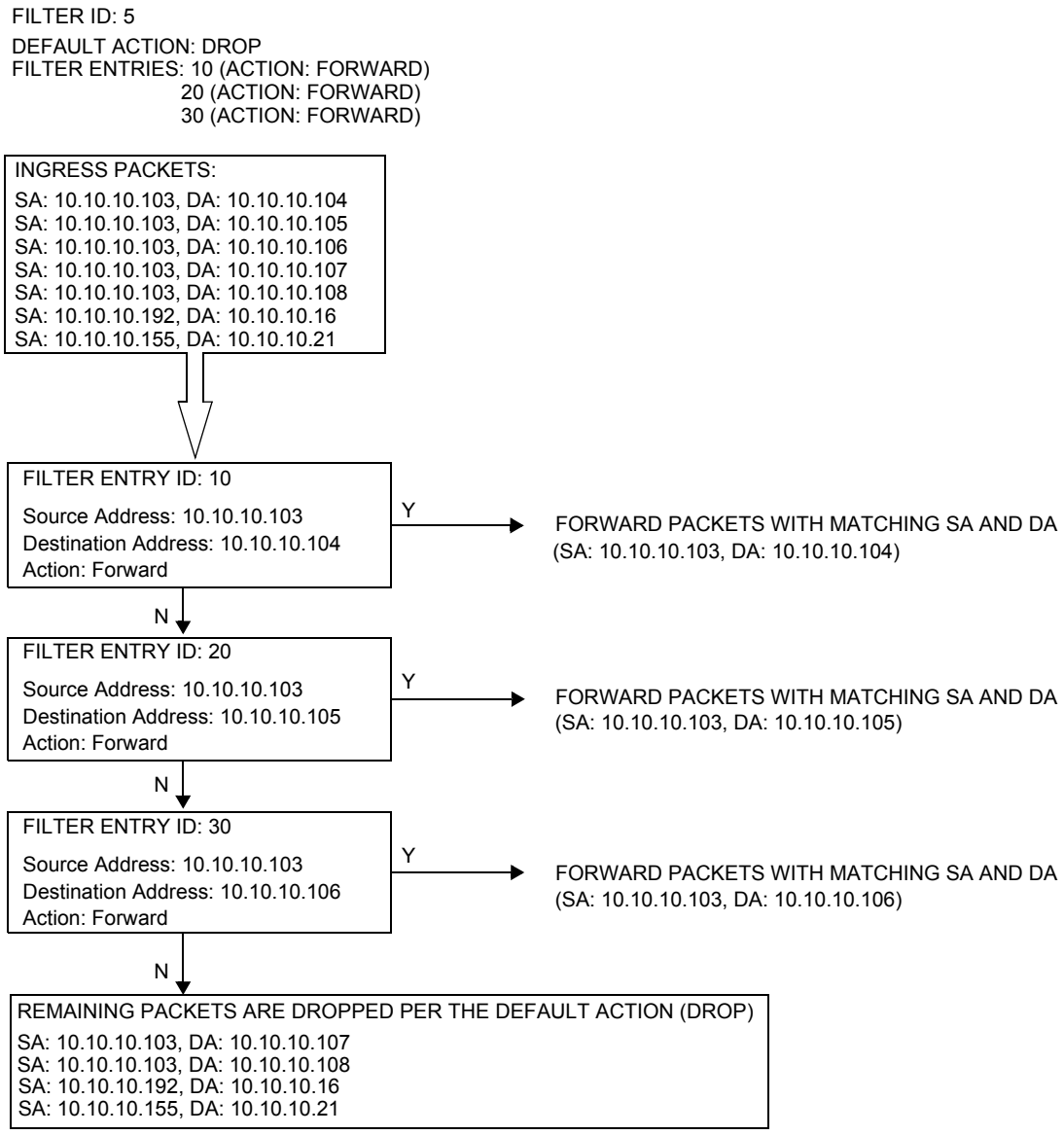
- If a packet matches all the entry criteria, the entry's specified action is performed (drop or forward).
- If a packet does not match all of the entry criteria, the policy's default action is performed (drop).

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, then the default action is performed (drop).

Figure 7 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

Figure 7: Filtering Process Example



Applying Filters to a Network Port

You can apply an IP filter to a network port. Packets received on the interface are checked against the matching criteria in the filter entries. If the packet completely matches all criteria in an entry, the checking stops. If permitted, the traffic is forwarded. If the packets do not match, they are discarded.

Configuration Notes

The following information describes filter implementation caveats.

- Creating a filter policy is optional.
- Associating a service with 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 ports, packets are compared to the criteria specified within the entry or entries.
- When you configure a large (complex) filter, it take may 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.

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 179.

Configuring Filter Policies with CLI

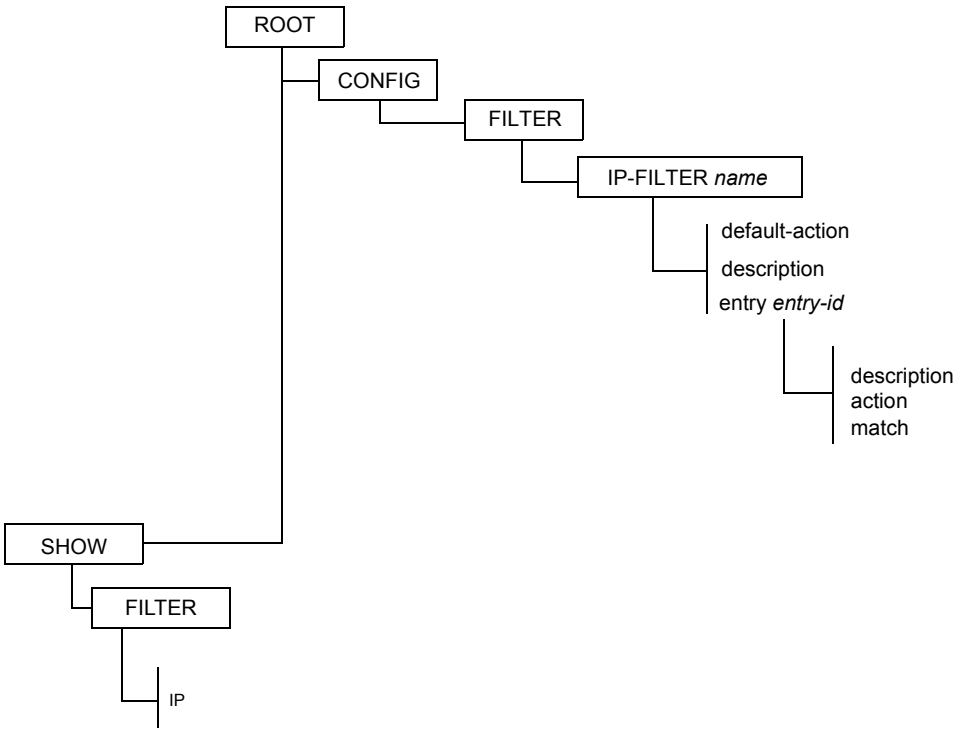
This section provides information to configure and manage filter policies using the command line interface.

Topics in this section include:

Filter CLI Command Structure

Figure 8 displays the 7705 SAR OS filter command structure. The filter configuration commands are located under the `config>filter` context and the show commands are under `show>filter`.

Figure 8: Filter Command Structure



List of Commands

Table 17 lists all the filter configuration commands, indicating the configuration level at which each command is implemented with a short command description. The filter policy command list is organized in the following task-oriented manner:

- Configure an IP filter policy
- Configure an IP filter policy entry
- Configure IP filter entry matching criteria

Table 17: CLI Commands to Configure Filter Policies Parameters

Command	Description	Page
Configure an IP filter policy		
`config>filter`		
`ip-filter`	Creates an IP filter policy	121
`default-action`	The default action specifies the action to be applied to packets when the packets do not match the specified criteria in any of the IP filter entries of the filter. The default action is always Drop; it cannot be reconfigured.	122
`description`	A text string describing the filter policy	120
`renum`	Renumbers existing filter entries to properly sequence filter entries	122
`scope`	Configures the filter policy scope as exclusive or template. An exclusive policy can only be applied to a single entity (network port). A template policy can be applied to multiple network ports.	123
Configure an IP filter policy entry		
`config>filter>ip-filter`		
`entry`	Creates a filter entry and identifies a group of match criteria and the corresponding action	124
`action`	Creates the drop or forward action associated with the match criteria. If not specified, the filter policy entry is not taken into account.	125
`description`	A text string describing the entry	120
Configure IP filter entry matching criteria		
`config>filter>ip-filter>entry`		
`match`	Enables the context to configure match criteria for the filter entry	125
`dst-ip`	Configures a destination IP address range to be used for IP filter matching	128

Table 17: CLI Commands to Configure Filter Policies Parameters (Continued)

Command	Description	Page
dst-port	Configures a destination TCP or UDP port number or port range for IP filter matching	128
icmp-code	Configures matching on ICMP code field in the ICMP header of an IP packet for IP filter matching.	129
icmp-type	Configures matching on ICMP type field in the ICMP header of an IP packet for IP filter matching.	129
src-ip	Configures a source IP address range to be used for IP filter matching	130
src-port	Configures a source TCP or UDP port number or port range for IP filter matching	130

Basic Configuration

The most basic IP filter policy must have the following:

- a filter ID
- template scope, either *exclusive* or *template*
- default action (always drop)
- 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.

To configure a filter policy, perform the following tasks:

- Creating an IP Filter Policy
- Applying Filter Policies to Network Ports

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 (always drop)
- 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
    dst-ip {ip-address/mask|ip-address netmask}
    dst-port {{lt|gt|eq} dst-port-number} | {range start
       end}
    icmp-code icmp-code
    icmp-type icmp-type
    src-ip {ip-address/mask|ip-address netmask}
    src-port {{lt|gt|eq} dst-port-number} | {range start
       end}
```

Example:
```
config>filter>ip-filter>entry# match
config>filter>ip-filter>entry>match# src-ip
   10.10.10.103/24
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 10.10.10.103/24
                exit
                action forward exit
----------------------------------------------
A:ALU-7>config>filter>ip-filter#
```

Applying Filter Policies to Network Ports

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
```

```
A:ALU-48>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
...
        interface "to-104"
            address 10.0.0.103/24
            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 20 10
config>filter>ip-filter# renum 40 1
```

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

```
A:ALU-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 20 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 30 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 10.10.10.91/24
                    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 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
        exit
...
----------------------------------------------
A:ALU-7>config>filter#
```

Modifying 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 10.10.10.91/24
                    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 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 30 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

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
            — renum old-entry-id new-entry-id
            — scope {exclusive | template}
            — no scope
            — entry entry-id [create]
            — no entry entry-id
                — action [drop | forward]
                — no action
                — description description-string
                — no description
                — match [protocol protocol-id]
                — no match
                    — 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
                    — icmp-code icmp-code
                    — no icmp-code
                    — icmp-type icmp-type
                    — no icmp-type
                    — 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
```

Show Commands

show
— **filter**
— **ip** [*ip-filter-id*] [**entry** *entry-id*] [**association** | **counters**]

Clear Commands

clear
— **filter**
— **ip** *ip-filter-id* [**entry** *entry-id*] [**ingress**]

Monitor Commands

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

Configuration Commands

Generic Commands

description

Syntax **description** *string*
no description

Context config>filter>ip-filter
config>filter>ip-filter>entry

Description This command creates a text description for a configuration context to help identify the content in the configuration file.

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

Default **none**

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

Global Filter Commands

ip-filter

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

Context config>filter

Description This command creates a configuration context for an IP filter policy.

IP filter policies specify either a forward or a drop action for packets based on the specified match criteria.

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.

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

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

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

Values 1 to 65535

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

Filter Policy Commands

default-action

Syntax **default-action drop**

Context config>filter>ip-filter

Description This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP filter entries of the filter. The default action is always to drop the packets. This parameter cannot be reconfigured.

Default **drop**

Parameters **drop —** specifies that all packets will be dropped unless there is a specific filter entry that causes the packet to be forwarded

renum

Syntax **renum** *old-entry-id new-entry-id*

Context config>filter>ip-filter

Description This command renumbers existing IP filter entries to properly sequence filter entries.

This may be required in some cases since the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-id* — the entry number of an existing entry

Values 1 to 30

new-entry-id — the new entry number to be assigned to the old entry

Values 1 to 30

scope

Syntax **scope** {**exclusive** | **template**}
no scope

Context config>filter>ip-filter

Description This command configures the filter policy scope as exclusive or template. If the scope of the policy is template and is applied to one or more network interfaces, the scope cannot be changed.

The **no** form of the command sets the scope of the policy to the default of **template**.

Default **template**

Parameters **exclusive —** when the scope of a policy is defined as exclusive, the policy can only be applied to a single entity (network port). If an attempt is made to assign the policy to a second entity, an error message will result. If the policy is removed from the entity, it will become available for assignment to another entity.

template — when the scope of a policy is defined as template, the policy can be applied to multiple network ports

General Filter Entry Commands

entry

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

Context config>filter>ip-filter

Description This command creates or edits an IP filter entry. Multiple entries can be created using unique entry-id numbers within the filter. The 7705 SAR implementation exits the filter on the first match found and executes the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.

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

The **no** 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.

Default **none**

Parameters *entry-id* — an entry-id uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 30

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

IP Filter Entry Commands

action

Syntax **action** {**drop | forward**}
no action

Context config>filter>ip-filter>entry

Description This command specifies what action to take (drop or forward) if the packets match the entry criteria. The **action** keyword must be entered and a keyword specified in order for the entry to be active.

Multiple action statements entered will overwrite previous action parameters when defined.

The **no** form of the command removes the specified **action** statement. The filter entry is considered incomplete and hence rendered inactive without the **action** keyword.

Default **none**

Parameters **drop** — specifies that packets matching the entry criteria will be dropped

forward — specifies that packets matching the entry criteria will be forwarded

If neither drop nor forward is specified, the filter action is No-Op and the filter entry is inactive.

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, hexidecimal, 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
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP

Protocol	Protocol ID	Description
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

IP Filter Match Criteria Commands

dst-ip

Syntax **dst-ip** {*ip-address*/*mask* | *ip-address netmask*]
no dst-ip

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

Description This command configures a destination IP address range to be used as an IP filter match criterion.

To match on the destination IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

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

Default **none**

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 quad notation

Values 0.0.0.0 to 255.255.255.255

dst-port

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

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

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

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

Default **none**

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

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

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

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

dst-port-number — the destination port number to be used as a match criteria expressed as a decimal integer

Values 1 to 65535

range *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

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

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

src-ip

Syntax **src-ip** {*ip-address*/*mask* | *ip-address netmask*]
no src-ip

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

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

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.

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 quad 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

range *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

Show Commands

ip

Syntax **ip** [*ip-filter-id*] [**entry** *entry-id*] [**association** | **counters**]

Context show>filter

Description Displays IP filter information.

Parameters *ip-filter-id* — displays detailed information for the specified filter ID and its filter entries

Values 1 to 65535

entry *entry-id* — displays information on the specified filter entry ID for the specified filter ID only

Values 1 to 30

associations — appends information as to where the filter policy ID is applied to the detailed filter policy ID output

counters — displays counter information for the specified filter ID

Output **Filter Output —** The following tables list filter output fields.

- Table 18: Show Filter Output Fields
- Table 19: Show Filter Output Fields (Filter ID Specified)
- Table 20: Show Filter Associations Output Fields
- Table 21: Show Filter Counters Output Fields

Table 18: 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
===============================================================================
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 (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, then the filter entry is incomplete as no action has been specified.
Description	The IP filter policy description
Src. IP	The source IP address and prefix length match criterion
Dest. IP	The destination IP address and prefix length match criterion
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.

Table 19: Show Filter Output Fields (Filter ID Specified) (Continued)

Label	Description
Match action	Default — the filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates that the entry is 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-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 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.
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-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 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

Table 21: Show Filter Counters Output Fields (Continued)

Label	Description
Entry	The filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Ing. Matches	The number of ingress filter matches/hits for the filter entry

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#
```

Clear Commands

ip

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

Context clear>filter

Description Clears the counters associated with the IP filter policy.

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.

Default **Clears all counters associated with the IP filter policy entries.**

Parameters *ip-filter-id* — the IP filter policy ID

Values 1 to 65535

entry-id — only the counters associated with the specified filter policy entry will be cleared

Values 1 to 30

ingress — only the ingress counters will be cleared

Monitor Commands

filter

Syntax **filter ip** *ip-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors the counters associated with the IP filter policy.

Parameters *ip-filter-id* — the IP filter policy ID

Values 1 to 65535

entry-id — only the counters associated with the specified filter policy entry will be monitored

Values 1 to 30

interval — configures the interval for each display in seconds

Values 3 to 60

Default 5 seconds

repeat *repeat* — configures how many times the command is repeated

Values 1 to 999

Default 10

absolute — when the **absolute** keyword is specified, the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.

rate — when the **rate** keyword is specified, 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

In Release 1.1, route policies are mainly used to manage the label database. Route policies can be used to configure which labels should be learned or advertised. Labels from a peer can be configured, and labels advertised by certain peers can be discarded.

There are no default route policies. Each policy must be created explicitly and applied. Policy parameters are modifiable.

Label learning and forwarding of MPLS packets are based on the defined policies, if there are any. If no route policies are defined, all advertised labels received from peers are learned and accepted. In Release 1.1 of the 7705 SAR, only static IP routing is supported (that is, no dynamic routing protocols are supported in this release).

Policy Statements

Route policies contain policy statements containing ordered entries that contain match conditions and actions that you specify. The entries should be sequenced from the most explicit to the least explicit.

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. You can specify matching criteria based on source or particular properties of a route.

You can also provide more matching conditions by specifying criteria such as:

- Prefix list — a named list of prefixes
- From criteria — a route's 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 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, then 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, then the default action is used.
- If a default action is defined and one or more matches occurred with the entries of the policy, then 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:

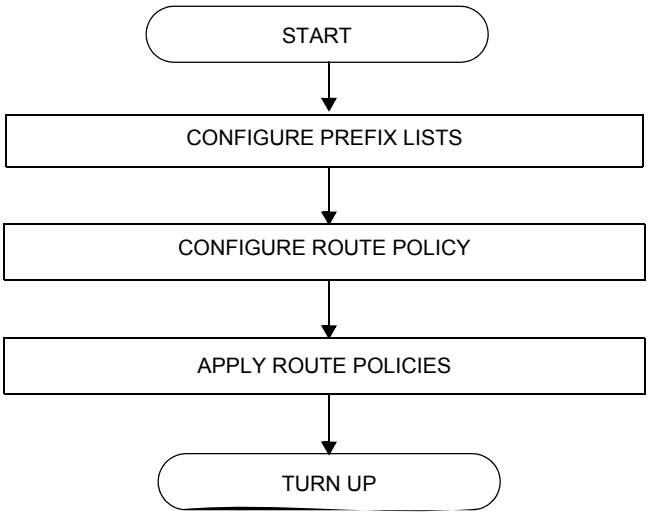
- 0.0.0.0/8 or longer
- 127.0.0.0/8 or longer
- 224.0.0.0/4 or longer
- 240.0.0.0/4 or longer

Any other prefixes that need to be filtered can be filtered explicitly using route policies.

Route Policy Configuration Process Overview

Figure 9 displays the process to provision basic route policy parameters.

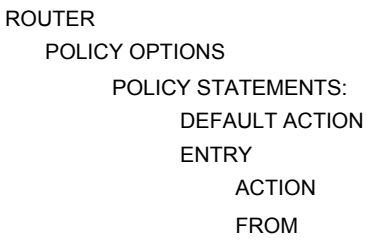
Figure 9: Route Policy Configuration and Implementation Flow



Route Policy Configuration Components

Figure 10 displays the major components to configure route policies.

Figure 10: Route Policy Configuration Components



- Policy options — define the parameters to configure route policies. Route policies are applied to the router interface.
- Policy statements — a logical grouping of match and action criteria that controls the flow of routing information from a particular neighbor
- Default action — the action for routes that do not match any policy entries
- Action — the action for routes matching a policy entry
- From — configure policy match criteria based on source of routes from which it is received

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 179.

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

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.

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.

In Release 1.1, the 7705 SAR supports simple route policy configuration.

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.

In Release 1.1, route policies are mainly used to manage the label database. Route policies can be used to configure which labels should be learned or advertised. Labels from a peer can be configured, and labels advertised from certain peers can be discarded.

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.

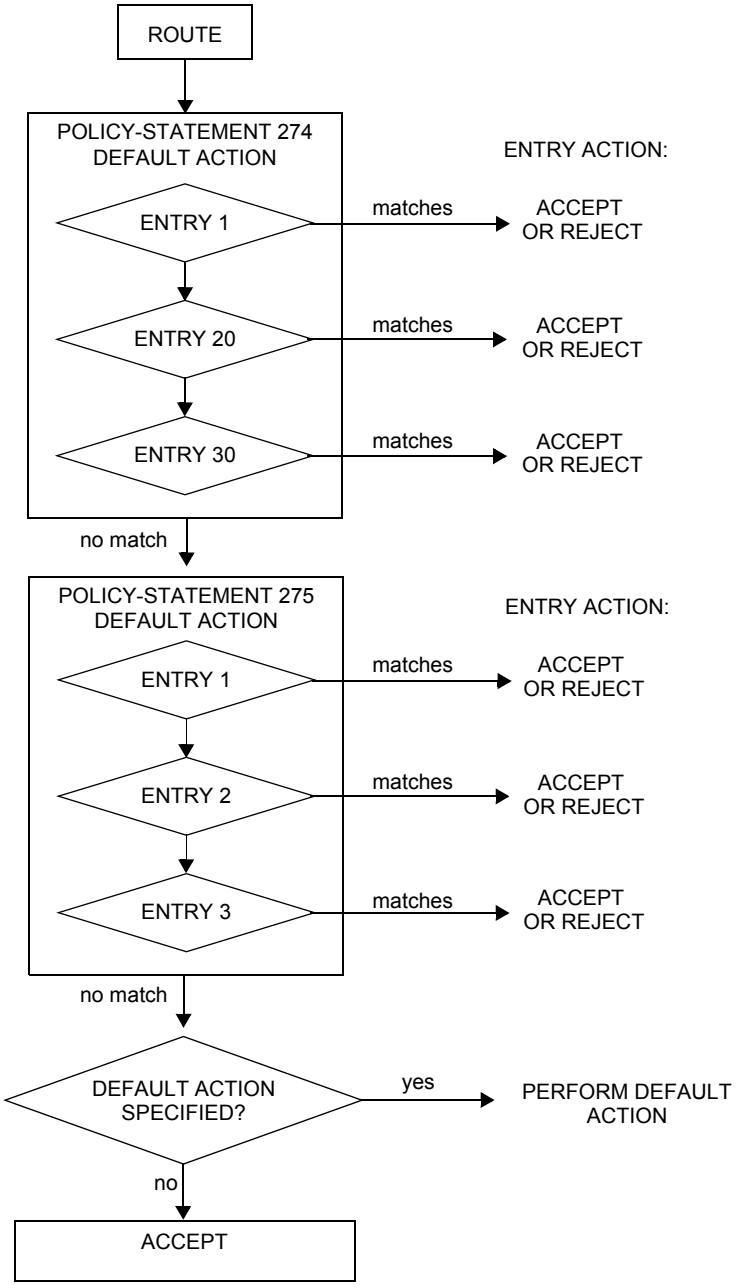
Each route policy statement can have a default-action clause defined. If a default-action is defined for one or more of the configured route policies, then the default actions should be handled in the following ways.

- 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, then 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 11 depicts an example of the route policy process.

Figure 11: Route Policy Process Example



Route Policy CLI Command Structure

The 7705 SAR route policy command structure is displayed in Figure 13. Policy configuration commands are located under the `config>router>policy-options` context.

Figure 12: 7705 SAR OS Route Policy Command Structure

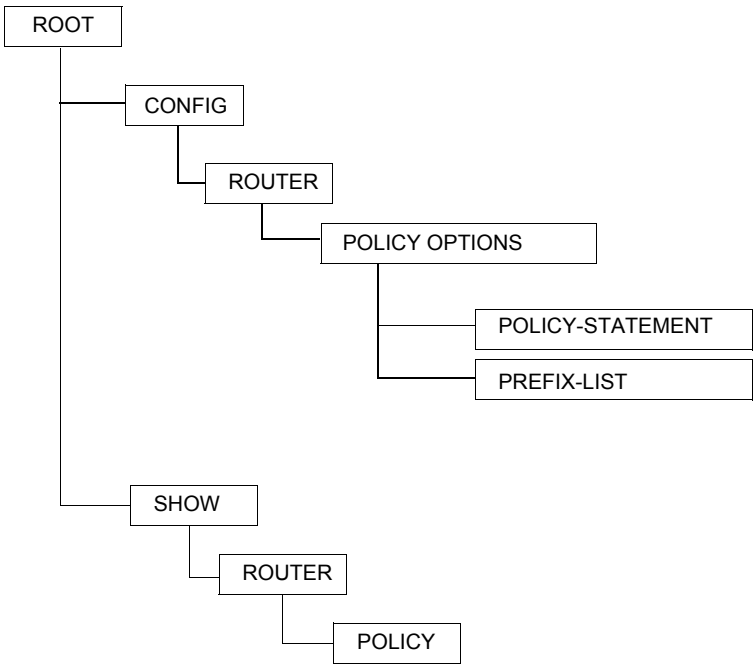
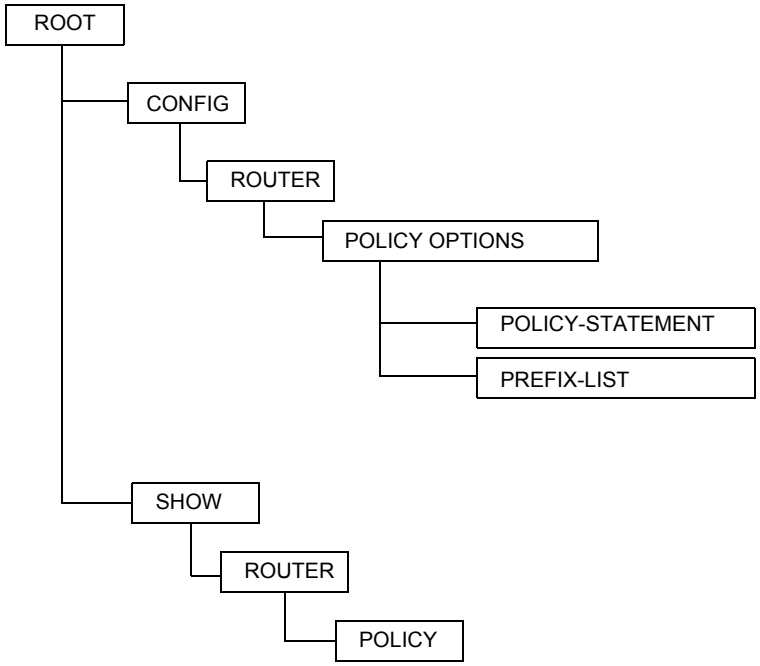


Figure 13: 7705 SAR OS Route Policy Command Structure



List of Commands

Table 22 lists all the route policy configuration commands, indicating the configuration level at which each command is implemented with a short command description. The route policy command list is organized in the following task-oriented manner:

- Begin a policy statement
- Create a policy statement
- Configure a policy statement
- Configure a prefix list
- Configure an entry and action statements
- Configure 'from' parameters

Table 22: CLI Commands to Configure Route Policy Parameters

Command	Description	Page
Begin a policy statement		
`config>router>policy-options`		
`begin`	Enter this keyword in order to enter the mode to create or edit route policies	167
`commit`	Enter this keyword in order to save the changes made to route policies during a session	167
`abort`	Enter this keyword in order to discard the changes that have been made to route policies during a session	167
Create a policy statement		
`config>router>policy-options`		
`policy-statement`	Creates a route policy statement	169
Configure a policy statement		
`config>router>policy-options>policy-statement`		
`default-action`	Creates the context for configuring actions for routes that do not match any route policy statement entries	175
`description`	Creates a text description stored in the configuration file for a configuration context	168

Table 22: CLI Commands to Configure Route Policy Parameters (Continued)

Command	Description	Page
Configure a prefix list		
`config>router>policy-options`		
`prefix-list`	Creates the context for configuring a prefix list for use in route policy entries	170
`prefix`	Creates a prefix entry in the route policy prefix list	170
Configure an entry and action statements		
`config>router>policy-options>policy-statement`		
`entry`	Creates the context for editing route policy entries within the route policy statement	172
`action`	Creates the context for configuring actions to take for routes matching a route policy statement entry	175
`description`	Text string to describe the default action entry	168
Configure 'from' parameters		
`config>router>policy-options>policy-statement>entry`		
`from`	Creates the context for configuring policy match criteria based on a route's source. If no condition is specified, all route sources are considered to match.	172
`neighbor`	Configures a neighbor or prefix list as a match criterion for a route policy statement entry. If no neighbor is specified, any neighbor is considered a match.	173
`prefix-list`	Configures a prefix list as a match criterion for a route policy statement entry. If no prefix list is specified, any network prefix is considered a match.	173

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.

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------

            policy-statement "Specifyprefixlist"
                entry 1
                    from
                        prefix-list "list1"
                    exit
                    action accept
                    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 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 on page 159).

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

CLI Syntax:

```
config>router> policy-options
begin
commit
abort
policy-statement name
     default-action {accept|next-entry|next-
        policy|reject}
```

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
                exit
            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
           neighbor {ip_addr|prefix-list name}
           prefix-list name [name [name [name [name]]]]
```

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$ from
policy-statement>entry>from# neighbor 10.10.10.104
policy-statement>entry>from# 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# neighbor 10.10.0.91
policy-statement>entry>from# exit
policy-statement>entry# from
policy-statement>entry>from$ prefix-list list2
policy-statement>entry>from# 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
                    from
                        neighbor 10.10.10.104
                    exit
                    action accept
                    exit
                exit
                entry 2
                   from
                        prefix-list list2
                   exit
                   from
                        neighbor 10.10.0.91
                    exit
                    action accept
                    exit
                exit
                default-action accept
                    . . .
                exit
            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

```
config
    — [no] router
        — [no] policy-options
            — begin
            — commit
            — abort
            — [no] policy-statement name
                — description description-string
                — no description
                — default-action {accept | next-entry | next-policy | reject}
                — no default-action
                — entry entry-id
                — no entry
                    — description description-string
                    — no description
                    — action {accept | next-entry | next-policy | reject}
                    — no action
                    — [no] from
                        — neighbor {ip-address | prefix-list name}
                        — no neighbor
                        — prefix-list name [name...(up to 5 max)]
                        — no prefix-list
            — [no] prefix-list name
                — [no] prefix ip-prefix/mask [exact | longer | through length | prefix-
                  length-range length1-length2]
```

Show Commands

```
show
    — router router-name
        — policy [name | prefix-list name | admin]
```

Configuration Commands

Generic Commands

abort

Syntax **abort**

Context config>router>policy-options

Description This command discards changes made to a route policy.

Default **none**

begin

Syntax **begin**

Context config>router>policy-options

Description This command enters the mode to create or edit route policies.

Default **none**

commit

Syntax **commit**

Context config>router>policy-options

Description This command saves changes made to a route policy.

Default **none**

description

Syntax **description** *string*
no description

Context config>router>policy-options>policy-statement
config>router>policy-options>policy-statement>entry

Description This command creates a text description that is stored in the configuration file to help identify the content of the entity.

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

Default **none**

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

Route Policy Options

policy-options

Syntax [**no**] **policy-options**

Context config>router

Description This command enables the context to configure route policies. Route policies are applied to the routing protocol.

The **no** form of the command deletes the route policy configuration.

Default **none**

policy-statement

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

Context config>router>policy-options

Description This command creates the context to configure a route policy statement.

Route policy statements control the flow of routing information from a specific protocol or protocols.

The **policy-statement** is a logical grouping of match and action criteria. A single **policy-statement** can affect routing in one or more protocols and/or one or more protocols' peers/neighbors. A single **policy-statement** can also affect the export of routing information.

The **no** form of the command deletes the policy statement.

Default **no policy-statement** — No route policy statements are defined.

Parameters *name* — 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.

Route Policy Prefix Commands

prefix-list

Syntax [**no**] **prefix-list** *name*

Context config>router>policy-options

Description This command creates a context to configure a prefix list to use in route policy entries.

The **no** form of the command deletes the named prefix list.

Default **none**

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.

prefix

Syntax [**no**] **prefix** *ip-prefixImask* [**exact** | **longer** | **through** *length* | **prefix-length-range** *length1-length2*]

Context config>router>policy-options>prefix-list

Description This command creates a prefix entry in the route policy prefix list.

The **no** form of the command deletes the prefix entry from the prefix list.

Parameters *ip-prefix* — the IP prefix for the prefix list entry in dotted decimal notation

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

mask — the IP prefix length

Values 0 to 32

exact — specifies that the prefix list entry only matches the route with the specified *ip-prefix* and *mask* (prefix length) values

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

through *length* **—** specifies that the prefix list entry matches any route that matches the specified *ip-prefix* and has a *mask* value within the specified *length* values

Values 0 to 32

prefix-length-range *length1* **-** *length2* **—** specifies that a route must match the most significant bits and have a mask value within the given range

Values 0 to 32, *length2* > *length1*

Route Policy Entry Match Commands

entry

Syntax **entry** *entry-id*
no entry

Context config>router>policy-options>policy-statement *name*

Description This command creates the context to edit route policy entries within the route policy statement.

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.

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.

The **no** form of the command removes the specified entry from the route policy statement.

Default **none**

Parameters *entry-id* — the entry ID expressed as a decimal integer. An *entry-id* uniquely identifies match criteria and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 4294967295

from

Syntax [**no**] **from**

Context config>router>policy-options>policy-statement>entry

Description 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.

If no condition is specified, all route sources are considered to match.

The **no** form of the command deletes the source match criteria for the route policy statement entry.

neighbor

Syntax **neighbor** {*ip-address* | **prefix-list** *name*}
no neighbor

Context config>router>policy-options>policy-statement>entry>from

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 of the command removes the neighbor IP match criterion from the configuration.

Default **no neighbor** — matches any neighbor

Parameters *ip-address* — the neighbor IP address in dotted decimal notation

Values *ip-address* a.b.c.d

prefix-list *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.

The *name* specified must already be defined.

prefix-list

Syntax **prefix-list** *name* [*name*...up to 5 max]
no prefix-list

Context config>router>policy-options>policy-statement>entry>from

Description This command configures a prefix list as a match criterion for a route policy statement entry.

If no prefix list is specified, any network prefix is considered a match.

The prefix lists specify the network prefix (this includes the prefix and length) that a specific policy entry applies to.

Up to five prefix list names can be specified.

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

Default **no prefix-list** — matches any network prefix

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.

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

Route Policy Action Commands

action

Syntax **action** {**accept | next-entry | next-policy | reject**}
no action

Context config>router>policy-options>policy-statement>entry

Description This command creates the context to configure actions to take for routes matching a route policy statement entry.

This command is required and must be entered for the entry to be active.

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 — specifies that 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 — specifies that 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 — specifies that routes matching the entry match criteria will be rejected

default-action

Syntax **default-action** {**accept** | **next-entry** | **next-policy** | **reject**}
no default-action

Context config>router>policy-options>policy-statement *name*

Description This command enables the context to configure actions for routes that do not match any route policy statement entries when the **accept** parameter is specified.

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, then the policy evaluation terminates and the appropriate result is returned.

If a default action is defined and no match(es) occurred with the entries in the policy, then the default action clause is used.

If a default action is defined and one or more matches occurred with the entries of the policy, then the default action is not used.

The **no** form of the command deletes the **default-action** context for the policy statement.

Default **no default-action**

Parameters **accept —** specifies that routes matching the entry match criteria will be accepted and propagated

next-entry — specifies that 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 — specifies that 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 — specifies that routes matching the entry match criteria will be rejected

Show Commands

policy

Syntax **policy** [*name* | **prefix-list** *name* | **admin**]

Context show>router

Description This command displays configured policy statement information.

Parameters *name* — if a *name* is specified, the matching policy statement is displayed. If no name is specified, a list of all policy statements and descriptions are displayed.

prefix-list — displays the prefix lists configured in the route policy

admin — if the keyword **admin** is included, the entire policy option configuration is displayed, including any uncommitted configuration changes. This command is similar to the **info** command.

Output **Route Policy Output —** The following table describes route policy output fields.

Table 23: Show Route Policy Output Fields

Label	Description
`Policy`	Displays a list of route policy names
`Description`	Displays the description of each route policy
`Policies`	The total number of policies configured

Standards and Protocol Support

Standards Compliance

IEEE 802.1p/q VLAN Tagging
IEEE 802.3 10BaseT
IEEE 802.3u 100BaseTX
IEEE 802.3x Flow Control
IEEE 802.3z 1000BaseSX/LX

Protocol Support

LDP

RFC 5036 LDP Specification

MPLS

RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

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

TCP/IP

RFC 768 UDP
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1350 The TFTP Protocol (Rev. 2)
RFC 1812 Requirements for IPv4 Routers

PPP

RFC 1332 PPP IPCP
RFC 1661 PPP
RFC 1662 PPP in HDLC-like Framing
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)

ATM

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

PSEUDOWIRES

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 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RADIUS

RFC 2865 Remote Authentication Dial In User Service

RFC 2866 RADIUS Accounting

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

TACACS+

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

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

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 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 2138 RADIUS

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 2665 EtherLike-MIB

RFC 2819 RMON-MIB

RFC 2863 IF-MIB

RFC 2864 INVERTED-STACK-MIB

RFC 3014 NOTIFICATION-LOG MIB

RFC 3164 The BSD Syslog Protocol

RFC 3273 HCRMON-MIB

RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413 Simple Network Management Protocol (SNMP) Applications

RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3418 SNMP MIB

draft-ietf-disman-alarm-mib-04.txt

draft-ietf-mpls-ldp-mib-07.txt

IANA-IFType-MIB

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-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/osds

Product manuals and documentation updates are available through the Alcatel-Lucent Support Documentation and Software Download service at 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

Customer documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 04297 AAAA TQZZA Edition 01